

# **ZENworks Control Center Reference**

## **ZENworks® 11 Support Pack 2**

July 02, 2012

## Legal Notices

Novell, Inc., makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc., reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc., makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc., reserves the right to make changes to any and all parts of Novell software, at any time, without any obligation to notify any person or entity of such changes.

Any products or technical information provided under this Agreement may be subject to U.S. export controls and the trade laws of other countries. You agree to comply with all export control regulations and to obtain any required licenses or classification to export, re-export or import deliverables. You agree not to export or re-export to entities on the current U.S. export exclusion lists or to any embargoed or terrorist countries as specified in the U.S. export laws. You agree to not use deliverables for prohibited nuclear, missile, or chemical biological weaponry end uses. See the [Novell International Trade Services Web page \(http://www.novell.com/info/exports/\)](http://www.novell.com/info/exports/) for more information on exporting Novell software. Novell assumes no responsibility for your failure to obtain any necessary export approvals.

Copyright © 2007-2012 Novell, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

Novell, Inc.  
1800 South Novell Place  
Provo, UT 84606  
U.S.A.  
[www.novell.com](http://www.novell.com)

*Online Documentation:* To access the latest online documentation for this and other Novell products, see the [Novell Documentation Web page \(http://www.novell.com/documentation\)](http://www.novell.com/documentation/).

## Novell Trademarks

For Novell trademarks, see [the Novell Trademark and Service Mark list \(http://www.novell.com/company/legal/trademarks/tmlist.html\)](http://www.novell.com/company/legal/trademarks/tmlist.html).

## Third-Party Materials

All third-party trademarks are the property of their respective owners.

---

# About This Guide

This *ZENworks 11 SP2 ZENworks Control Center Reference* explains how to access, navigate, customize, and use ZENworks Control Center, the administrative console used to manage your ZENworks system. The guide includes the following sections:

- ♦ Chapter 1, “Accessing ZENworks Control Center,” on page 9
- ♦ Chapter 2, “Navigating ZENworks Control Center,” on page 13
- ♦ Chapter 3, “Customizing ZENworks Control Center,” on page 15
- ♦ Chapter 4, “Bookmarking ZENworks Control Center Locations,” on page 19
- ♦ Chapter 5, “Naming Objects in ZENworks Control Center,” on page 21
- ♦ Chapter 6, “Managing Administrators and Administrator Groups,” on page 23
- ♦ Chapter 7, “Organizing Devices into Folders and Groups,” on page 59
- ♦ Chapter 8, “Using Message Logging,” on page 65
- ♦ Chapter 9, “Customizing ZENworks News Alerts,” on page 81
- ♦ Chapter 10, “Using the Credential Vault,” on page 87
- ♦ Chapter 11, “Using Quick Tasks,” on page 93
- ♦ Chapter 12, “Using System Variables,” on page 99
- ♦ Chapter 13, “Using Special System Variables,” on page 103
- ♦ Chapter 14, “Troubleshooting ZENworks Control Center,” on page 117

## Audience

This guide is intended for ZENworks administrators.

## Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comments feature at the bottom of each page of the online documentation.

## Additional Documentation

ZENworks 11 SP2 is supported by other documentation (in both PDF and HTML formats) that you can use to learn about and implement the product. For additional documentation, see the [ZENworks 11 SP2 documentation Web site \(http://www.novell.com/documentation/zenworks11\)](http://www.novell.com/documentation/zenworks11).



---

# Contents

<b>About This Guide</b>	<b>3</b>
<b>1 Accessing ZENworks Control Center</b>	<b>9</b>
1.1 Accessing ZENworks Control Center . . . . .	9
1.2 Accessing ZENworks Control Center through Novell iManager . . . . .	10
<b>2 Navigating ZENworks Control Center</b>	<b>13</b>
<b>3 Customizing ZENworks Control Center</b>	<b>15</b>
3.1 Changing the Default Login Disable Values . . . . .	15
3.2 Changing the Timeout Value for ZENworks Control Center . . . . .	16
3.3 Using the Config.xml File to Modify ZENworks Control Center Settings . . . . .	17
<b>4 Bookmarking ZENworks Control Center Locations</b>	<b>19</b>
<b>5 Naming Objects in ZENworks Control Center</b>	<b>21</b>
<b>6 Managing Administrators and Administrator Groups</b>	<b>23</b>
6.1 Managing Administrator Accounts . . . . .	24
6.1.1 Creating Administrators . . . . .	24
6.1.2 Deleting Administrators . . . . .	25
6.1.3 Renaming Administrators . . . . .	25
6.1.4 Changing Administrator Passwords . . . . .	26
6.2 Managing Administrator Rights . . . . .	26
6.2.1 Assigning Super Administrator Rights . . . . .	26
6.2.2 Assigning Additional Rights . . . . .	27
6.2.3 Modifying Assigned Rights . . . . .	27
6.2.4 Removing Assigned Rights . . . . .	28
6.3 Managing Administrator Group Accounts . . . . .	28
6.3.1 Creating Administrator Group Account . . . . .	28
6.3.2 Creating Administrators . . . . .	30
6.3.3 Deleting Administrator Groups . . . . .	30
6.3.4 Renaming Administrator Groups . . . . .	31
6.4 Managing Administrator Group Rights . . . . .	31
6.4.1 Assigning Additional Rights . . . . .	31
6.4.2 Modifying Assigned Rights . . . . .	31
6.4.3 Removing Assigned Rights . . . . .	31
6.5 Rights Descriptions . . . . .	32
6.5.1 Administrator Rights . . . . .	33
6.5.2 Bundle Rights . . . . .	33
6.5.3 Contract Management Rights . . . . .	34
6.5.4 Credential Rights . . . . .	34
6.5.5 Deployment Rights . . . . .	35
6.5.6 Device Rights . . . . .	35
6.5.7 Discovery Rights . . . . .	36
6.5.8 Document Rights . . . . .	36

6.5.9	Inventoried Device Rights	37
6.5.10	LDAP Import Rights	38
6.5.11	License Management Rights	38
6.5.12	Location Rights	38
6.5.13	Patch Management Rights	38
6.5.14	Policy Rights	39
6.5.15	Quick Task Rights	40
6.5.16	Remote Management Rights	41
6.5.17	Reporting Rights	42
6.5.18	Subscription Rights	42
6.5.19	User Rights	42
6.5.20	ZENworks User Group Rights	43
6.5.21	Zone Rights	43
6.5.22	Inventory Report Rights	45
6.5.23	Asset Management Report Rights	45
6.6	Managing Administrator Roles	46
6.6.1	Understanding Administrator Roles	46
6.6.2	Creating a Role	50
6.6.3	Assigning Roles	51
6.6.4	Editing a Role	55
6.6.5	Renaming a Role	58
6.6.6	Deleting a Role	58

## **7 Organizing Devices into Folders and Groups** **59**

7.1	Folders	59
7.2	Groups	61
7.3	Assignment Inheritance for Folders and Groups	64

## **8 Using Message Logging** **65**

8.1	Functionalities of Message Logger	65
8.2	Message Severity	65
8.3	Message Format	66
8.4	Configuring Message Logger Settings	66
8.4.1	Configuring the Message Logger Settings at the Zone Level	66
8.4.2	Configuring the Message Logger Settings at the Folder Level	69
8.4.3	Configuring the Message Logger Settings at the Device Level	70
8.4.4	Turning on the Debug Messages	70
8.5	Managing Messages	70
8.5.1	Understanding Message Formats	71
8.5.2	Viewing the Message Status	73
8.5.3	Viewing the Messages	75
8.5.4	Acknowledging Messages	76
8.5.5	Deleting Messages	78
8.5.6	Viewing the Predefined Reports	80

## **9 Customizing ZENworks News Alerts** **81**

9.1	Managing ZENworks News Alerts	81
9.1.1	Deleting the News Alerts	82
9.1.2	Updating the News Alerts	82
9.1.3	Displaying the News Alerts Based on the Selected Category	82
9.1.4	Viewing the News	82
9.1.5	Sorting the News Alerts	82
9.2	Configuring ZENworks News Settings	82
9.2.1	Dedicated News Server	83
9.2.2	Schedule Type	84

<b>10 Using the Credential Vault</b>	<b>87</b>
10.1 Adding a Credential . . . . .	87
10.2 Creating a Folder for Credentials . . . . .	89
10.3 Assigning Credential Rights . . . . .	90
10.4 Editing a Credential . . . . .	90
10.5 Renaming a Credential . . . . .	91
10.6 Moving a Credential to Another Folder . . . . .	91
10.7 Removing a Credential. . . . .	91
<b>11 Using Quick Tasks</b>	<b>93</b>
11.1 Quick Tasks Types. . . . .	93
11.2 Initiating a Quick Task . . . . .	95
11.3 Cancelling, Stopping, or Hiding a Quick Task . . . . .	97
<b>12 Using System Variables</b>	<b>99</b>
12.1 Understanding System Variables . . . . .	99
12.2 Adding System Variables . . . . .	100
12.3 Removing System Variables . . . . .	101
12.4 Editing System Variables . . . . .	101
12.5 Using System Variables . . . . .	101
<b>13 Using Special System Variables</b>	<b>103</b>
13.1 Windows Special System Variables . . . . .	103
13.2 Login Script Special System Variables . . . . .	108
13.3 Novell eDirectory Attribute Special System Variables . . . . .	109
13.3.1 Syntax . . . . .	110
13.3.2 Examples . . . . .	110
13.3.3 Configuring the eDirectory Attribute Special System Variables . . . . .	111
13.4 Microsoft Active Directory Attribute Special System Variables . . . . .	112
13.4.1 Syntax . . . . .	112
13.4.2 Examples . . . . .	112
13.4.3 Configuring the Active Directory Attribute Special System Variables . . . . .	113
13.5 Language Variable Special System Variables . . . . .	114
<b>14 Troubleshooting ZENworks Control Center</b>	<b>117</b>





---

# 1 Accessing ZENworks Control Center

You use ZENworks Control Center to configure system settings and perform management tasks in your Management Zone.

ZENworks Control Center is installed on all ZENworks Servers in the Management Zone. You can perform all management tasks on any ZENworks Server.

- ♦ [Section 1.1, “Accessing ZENworks Control Center,” on page 9](#)
- ♦ [Section 1.2, “Accessing ZENworks Control Center through Novell iManager,” on page 10](#)

## 1.1 Accessing ZENworks Control Center

- 1 Using a Web browser that meets the requirements listed in “[Administration Browser Requirements](#)” in the *ZENworks 11 Installation Guide*, enter the following URL:

```
https://ZENworks_Server_Address:port
```

Replace *ZENworks\_Server\_Address* with the IP address or DNS name of the ZENworks Server. You only need to specify the *port* if you are not using one of the default ports (80 or 443). ZENworks Control Center requires an HTTPS connection; HTTP requests are redirected to HTTPS.

The login dialog box is displayed.



- 2 In the *Username* field, type Administrator (the default) or an administrator name that you [previously created](#) in ZENworks Control Center.

To log in to ZENworks Control Center as an administrator who has been created based on users in a user source who has the same name as a previously created ZENworks administrator, specify the username as *name@usersource*.

For example, if the administrator has the name `testadmin` and belongs to the user source named `myserver`, specify the username as `testadmin@myserver`.

- 3 In the *Password* field, do one of the following:
  - ♦ If you are logging in through the default Administrator account, specify the Administrator password that you created during installation.
  - ♦ Specify the password for the administrator name that you created in ZENworks Control Center.

To prevent unauthorized users from gaining access to ZENworks Control Center, the administrator account is disabled after three unsuccessful login attempts, and a 60-second timeout is enforced before you can attempt another login. To change these default values, see [Section 3.1, “Changing the Default Login Disable Values,” on page 15](#).

- 4 Click *Login* to display ZENworks Control Center.

To log in again as a different administrator, click the *Logout* option in the upper right corner of the ZENworks Control Center window, then when the login dialog box is displayed, log in as a different administrator.

## Performing concurrent operations in multiple sessions of ZENworks Control Center might result in an exception

If ZENworks Control Center is opened in multiple browsers and you choose to perform an operation on an object in one browser when the same object is being modified or accessed in the other browser, an exception might occur.

For example, an error might occur if you update an object in one session of ZENworks Control Center when the same object has been deleted in another session of ZENworks Control Center.

## 1.2 Accessing ZENworks Control Center through Novell iManager

ZENworks 11 SP2 includes a Novell plug-in module (`.npm`) that you can use to access ZENworks Control Center from Novell iManager, which is a management console used by many Novell products.

The ZENworks Control Center plug-in supports iManager 2.7 only. It does not support iManager 2.6 or 2.5; it will install to these versions but does not work.

To install the ZENworks Control Center plug-in for iManager:

- 1 On the server where iManager is located (or on a device that has access to the iManager server), open a Web browser to the ZENworks download page:  
`https://server/zenworks-setup`  
where *server* is the DNS name or IP address of a ZENworks Server.
- 2 In the left navigation pane, click *Administrative Tools*.
- 3 Click `zcc.npm` and save the file to a location on the iManager server.
- 4 Follow the instructions in the [Novell iManager 2.7 Administration Guide \(http://www.novell.com/documentation/imanager27/\)](http://www.novell.com/documentation/imanager27/) to install and configure the plug-in module.

- 5** Log into iManager.
- 6** Click the ZENworks icon at the top of the page.
- 7** Enter the ZENworks Control Center URL:

`https://ZENworks_Server_Address:port`

Replace *ZENworks\_Server\_Address* with the IP address or DNS name of the ZENworks Server.  
You only need to specify the *port* if the ZENworks server is not using the default port (80 or 443).

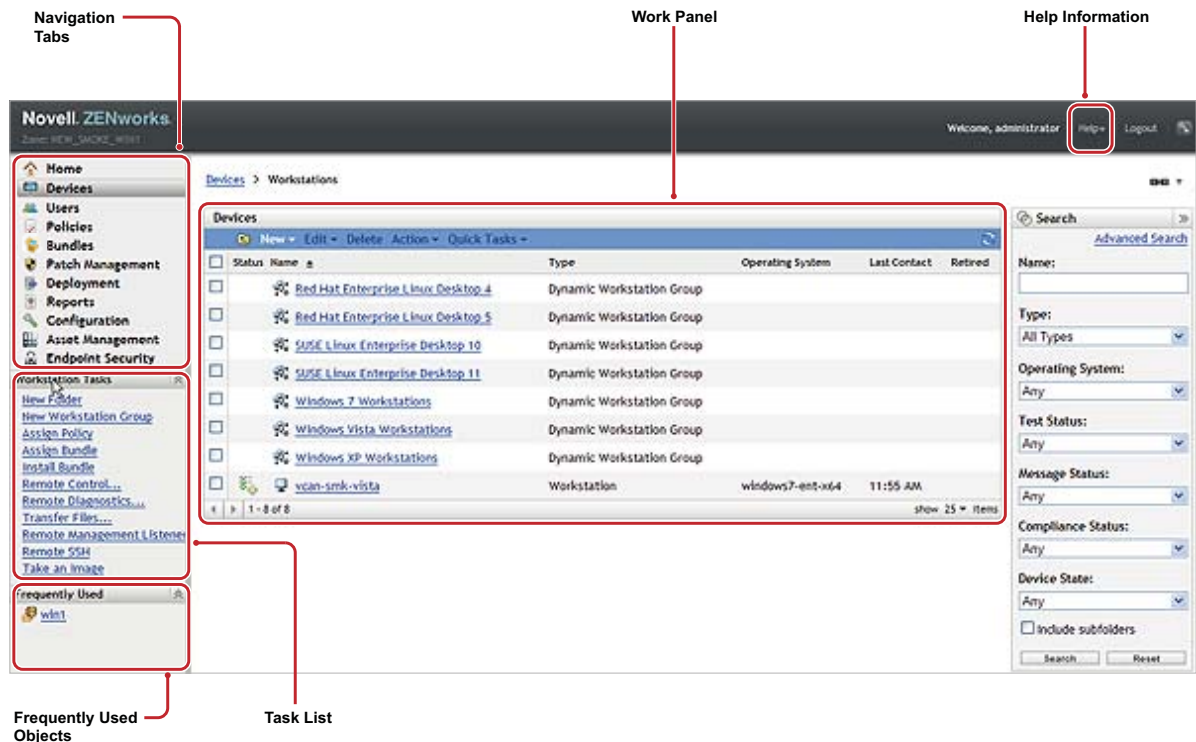
- 8** Click the ZENworks icon to launch ZENworks Control Center.



# 2 Navigating ZENworks Control Center

The following Workstations page represents a standard view in ZENworks Control Center:

**Figure 2-1** ZENworks Control Center



**Navigation Tabs:** The tabs in the left pane let you navigate among the functional areas of ZENworks. For example, the Servers page shown above lets you manage tasks associated with servers.

**Task List:** The task list in the left pane provides quick access to the most commonly performed tasks for the current page. The task list changes for each page. For example, the task list on the Bundles page displays bundle-related tasks and the task list on the Devices page displays device-related tasks.

**Frequently Used Objects:** The Frequently Used list in the left pane displays the 10 objects that you have accessed most often, from most used to least used. Clicking an object takes you directly to the details page for the object.

**Work Panel:** The work panels are where you monitor and manage your ZENworks system. The panels change depending on the current page. In the above example, there are two work panels: Devices and Search. The Devices panel lists the servers, folders, server groups, and dynamic server groups that have been created; you use this panel to manage the servers. The Search panel lets you filter the Devices panel based on criteria such as a device's name, operating system, or status.

**Help Information:** The *Help* button links to Help topics that provide information about the current page. The *Help* button links change depending on the current page.

---

# 3 Customizing ZENworks Control Center

You can change ZENworks Control Center settings to customize behavior such as the failed login timeout and the automatic logout timeout:

- ♦ [Section 3.1, “Changing the Default Login Disable Values,” on page 15](#)
- ♦ [Section 3.2, “Changing the Timeout Value for ZENworks Control Center,” on page 16](#)
- ♦ [Section 3.3, “Using the Config.xml File to Modify ZENworks Control Center Settings,” on page 17](#)

## 3.1 Changing the Default Login Disable Values

By default, an administrator’s account is disabled for 60 seconds after he or she unsuccessfully attempts to log in three times. You can change the number of login tries and the timeout length by editing a configuration file. The changes are only applied to the instance of ZENworks Control Center being run from the server where you open and modify the configuration file. To make the change applicable to all ZENworks Primary Servers, you must make the same change in each server’s copy of this file.

---

**IMPORTANT:** Login attempts per administrator account are maintained in the ZENworks database, and there is only one ZENworks database per Management Zone. Therefore, if a particular administrator unsuccessfully attempts to log in to one Primary Server, that administrator is locked out of all Primary Servers in the zone. The lockout period is determined by the configuration on the server where the login attempts failed.

---

To modify the login tries and timeout values:

- 1 In a text editor, open the following file:

**Windows:** `installation_location\novell\zenworks\conf\datamodel\zdm.xml`

**Linux:** `/etc/opt/novell/zenworks/datamodel/zdm.xml`

- 2 Add the following lines to the file:

```
<entry key="allowedLoginAttempts">5</entry>
```

```
<entry key="lockedOutTime">300</entry>
```

The 5 in this example represents the number of retries before disabling login, and 300 represents the number of seconds (the default is 60 seconds, or 1 minute).

Keep in mind that the longer the delay before allowing a re-login after the configured number of failures (such as 5), the longer your authorized administrators must wait to access ZENworks Control Center.

---

**IMPORTANT:** If you enter 0 as the login attempts value, the lockout functionality is disabled, allowing unlimited attempts at logging in.

---

- 3 Save the file, then restart the zenloader and zenserver services on the Primary Server to make the changes effective.

For instructions on restarting the services, see [“Restarting the ZENworks Services”](#) in the [ZENworks 11 SP2 Primary Server and Satellite Reference](#).

## 3.2 Changing the Timeout Value for ZENworks Control Center

By default, ZENworks Control Center has a 30-minute timeout value, so if you leave ZENworks Control Center idle on your computer for more than 30 minutes, you are prompted to log in again to continue.

The purpose of the timeout is to clear memory resources. The larger the timeout value, the longer ZENworks Control Center retains the memory resources, which might have a negative impact on the long-term performance of the device from which you have launched ZENworks Control Center, including the ZENworks Server if you have it running locally on it.

To increase or decrease the timeout value, you modify two XML files on the ZENworks Server. The change applies only to that server’s ZENworks Control Center. Therefore, any devices that launch ZENworks Control Center from that server experience the same timeout value.

You can make the ZENworks Control Center timeout value different on each ZENworks Server in the Management Zone.

To change the ZENworks Control Center timeout value on a ZENworks Server:

- 1 Open the `custom-config.xml` file in a text editor.

This file allows you to maintain customizations of ZENworks Control Center because information contained in this file overrides any corresponding information in the `config.xml` file. Therefore, changes made in this file are not lost when the `config.xml` file is overwritten during software updates or upgrades.

The `custom-config.xml` file is located in the same directory as the `config.xml` file:

- ♦ **Windows:** `\Novell\ZENworks\share\tomcat\webapps\zenworks\WEB-INF\custom-config.xml`
- ♦ **Linux:** `/opt/novell/zenworks/share/tomcat/webapps/zenworks/WEB-INF/custom-config.xml`

- 2 Locate the `<setting id="timeout">` entry.
- 3 Set the timeout value to the same number as you entered in the `config.xml` file.
- 4 Remove the comments surrounding the `<setting id="timeout">` entry (`<!--` and `-->`).
- 5 Save the `custom-config.xml` file.
- 6 Restart the ZENworks Server service.

For instructions, see [“Restarting the ZENworks Services”](#) in the [ZENworks 11 SP2 Primary Server and Satellite Reference](#)..



## 3.3 Using the Config.xml File to Modify ZENworks Control Center Settings

In addition to enabling you to configure the timeout value for the ZENworks Control Center (see [Section 3.2, “Changing the Timeout Value for ZENworks Control Center,” on page 16](#)), the `config.xml` file lets you control several additional configuration settings. However, with the exception of the timeout value, you should not need to modify the `config.xml` settings.

- 1 On the ZENworks Server, open the `config.xml` file in a text editor.
  - ♦ **Windows server path:** `\Novell\ZENworks\share\tomcat\webapps\ zenworks\WEB-INF\config.xml`
  - ♦ **Linux server path:** `opt/novell/zenworks/share/tomcat/webapps/zenworks/WEB-INF/config.xml`
- 2 Modify the desired setting. All settings begin with `<setting id=`.
  - timeout:** Specify the timeout value in minutes. The larger the timeout value, the longer ZENworks Control Center retains the memory resources, which might have a negative impact on the long-term performance of the device where you have launched ZENworks Control Center. If you change this value, you must also change the timeout entry in the `custom-config.xml` file. See [Section 3.2, “Changing the Timeout Value for ZENworks Control Center,” on page 16](#)).
  - debug.enabled:** Change the value to *false* if you do not want any messages written to the ZENworks Control Center log files. The default value, *true*, causes messages to be written to the log files.
  - debug.tags:** These settings control debug information. You should not change them unless instructed by Novell Support.
  - debug.log.viewstate:** This setting controls debug information. You should not change it unless instructed by Novell Support.
  - hideGettingStarted:** Suppresses the Getting Started page. This setting is not functional at this time. To manually suppress the page, open the ZENworks Control Center, display the Getting Started page, then select *Do not show me this again*.
  - noQuickTaskAutoRefresh:** This setting disables automatic refreshing of the QuickTask status dialog box. It is used to discover issues with QuickTask status updates. You should not change this setting unless instructed by Novell Support.
- 3 Save the `config.xml` file.
- 4 Restart the ZENworks Server service. See [“Restarting the ZENworks Services”](#) in the [ZENworks 11 SP2 Primary Server and Satellite Reference](#) for instructions.



---

# 4 Bookmarking ZENworks Control Center Locations

The Bookmark feature allows you to use your Web browser to manage direct access to the various locations in ZENworks Control Center, instead of performing the usual navigation clicks. You can also use this feature to bookmark hard-to-find locations.

You can create bookmarks for your Web browser to locations within the following sections of ZENworks Control Center:

- ♦ *Managed* tab on the *Devices* tab
- ♦ *Policies* tab
- ♦ *Bundles* tab
- ♦ *Management Zone Settings* on the *Configuration* tab

The locations you can bookmark include such items as lists, details of objects, and configuration settings.

Wherever the Link icon (🔗) is displayed, you can create a bookmark. The icon is located in the upper right of the page. If it is not displayed, a bookmark cannot be created for that location.

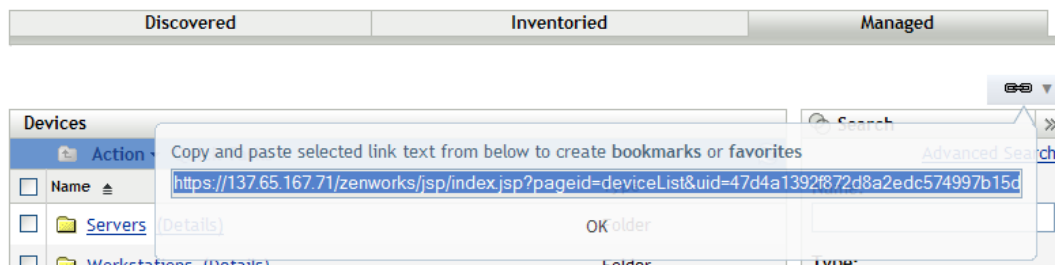
If you are logged in to ZENworks Control Center when you click a bookmark, the location is immediately displayed.

If you are not logged in to ZCC when you click a bookmark, the Login dialog box is displayed. After you enter valid credentials, the location is immediately displayed.

To create bookmarks:

- 1 In ZENworks Control Center, navigate to a location where you want to create a bookmark.
- 2 Click 🔗.

This opens the following dialog box, where the URL to the current location is already selected:



- 3 Press Ctrl+C to copy the URL, then click *OK* to close the dialog box.
- 4 Paste the URL as a new bookmark in your Web browser.



---

# 5 Naming Objects in ZENworks Control Center

When you name an object in the ZENworks Control Center (folders, bundles, policies, groups, registration keys, and so forth), ensure that the name adheres to the following conventions:

- ◆ The name must be unique in the folder.
- ◆ Depending on the database being used for the ZENworks database, uppercase and lowercase letters might not create uniqueness for the same name. The embedded database included with ZENworks 11 SP2 is case insensitive, so Folder 1 and FOLDER 1 are the same name and cannot be used in the same folder. If you use an external database that is case-sensitive, Folder 1 and FOLDER 1 are unique.
- ◆ If you use spaces, you must enclose the name in quotes when entering it on the command line. For example, you must enclose reg key 1 in quotes (“reg key 1”) when entering it in the zman utility.
- ◆ The following characters are invalid and cannot be used: / \ \* ? : " ' < > | ` % ~
- ◆ Ensure that the name of a bundle, policy, bundle folder, bundle group, policy folder, or policy group does not contain the following:
  - ◆ @Sandbox
  - ◆ @Version



---

# 6 Managing Administrators and Administrator Groups

During installation, a default ZENworks administrator account (named Administrator) is created. This account, called a Super Administrator account, provides full administrative rights to the Management Zone.

Typically, you should create administrator accounts for each person who will perform administrative tasks. You can define these accounts as Super Administrator accounts, or you can define them as administrator accounts with restricted rights. For example, you could give a user an administrator account that only enables him or her to discover and register devices in the Management Zone, the account could only enable the user to assign bundles to devices, or could limit the user to performing asset management tasks such as contract, license, and document management.

---

**IMPORTANT:** In addition to the default Administrator account, you should make sure that you have at least one other Super Administrator account. This provides redundancy in case the password for the Administrator account is forgotten or lost. For information on how to create a Super Administrator account, see [Section 6.2.1, “Assigning Super Administrator Rights,” on page 26](#). If you need any further help, contact [Novell Support \(http://www.novell.com/support\)](http://www.novell.com/support).

---

In some cases, you might have multiple administrator accounts that require the same administrative rights. Rather than assign rights to each account individually, you can create an administrator role, assign the administrative rights to the role, and then add the accounts to the role. For example, you might have a Help Desk role that provides administrative rights required by several of your administrators.

You can use administrator group that lets you group administrators so that you can assign rights and roles to groups rather than assigning rights and roles to individual administrators

To create and modify administrator accounts and assign roles, you can use ZENworks Control Center (ZCC) or the zman command line utility. If you prefer the zman command line utility, see [“Administrator Commands” in the ZENworks 11 SP2 Command Line Utilities Reference](#).

However, you can create and modify administrator group accounts and assign roles only through ZENworks Control Center (ZCC).

The following procedures explain how to create and modify administrators and administrator group accounts and assign roles through ZENworks Control Center (ZCC):

- ♦ [Section 6.1, “Managing Administrator Accounts,” on page 24](#)
- ♦ [Section 6.2, “Managing Administrator Rights,” on page 26](#)
- ♦ [Section 6.3, “Managing Administrator Group Accounts,” on page 28](#)
- ♦ [Section 6.4, “Managing Administrator Group Rights,” on page 31](#)
- ♦ [Section 6.5, “Rights Descriptions,” on page 32](#)
- ♦ [Section 6.6, “Managing Administrator Roles,” on page 46](#)

# 6.1 Managing Administrator Accounts

The following sections help you create and manage administrator accounts:

- ◆ Section 6.1.1, “Creating Administrators,” on page 24
- ◆ Section 6.1.2, “Deleting Administrators,” on page 25
- ◆ Section 6.1.3, “Renaming Administrators,” on page 25
- ◆ Section 6.1.4, “Changing Administrator Passwords,” on page 26

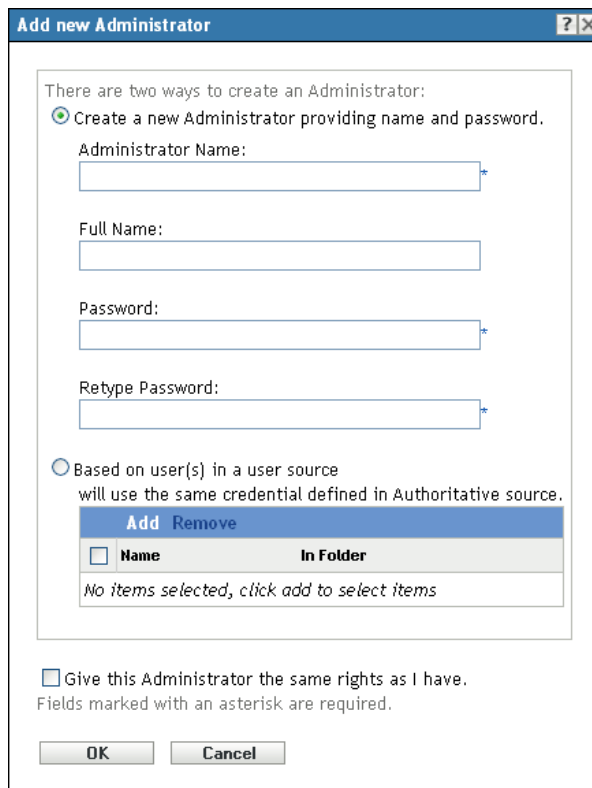
## 6.1.1 Creating Administrators

To create an administrator account:

- 1 In ZENworks Control Center, click the *Configuration* tab.



- 2 In the Administrators panel, click *New > Administrator* to display the Add New Administrator dialog box.





The Add New Administrator dialog box lets you create a new administrator account by providing a name and password, or you can create a new administrator based on an existing user in the user source. Optionally, you can give the new administrator the same rights that the logged-in administrator has.

**3** Fill in the fields:

**Create a New Administrator by Providing Name, Password:** Select this option if you want to create a new administrator account by manually specifying the name and password.

Administrator login names with Unicode characters are case-sensitive. Make sure that you use the correct case for each character in the login name when it contains Unicode characters.

The new administrator can change the password the first time he or she logs in by clicking the key icon located next to the *Logout* link in the upper right corner of ZENworks Control Center.

**Based on User(s) in a User Source:** Select this option if you want to create a new administrator account based on information from your user source. To do so, click *Add*, then browse for and select the user you want.

The newly created administrator account is granted View rights to all objects in the Management Zone. To grant additional rights, or to limit the administrator's rights to specific folders only, you need to [modify the rights](#).

**Give this Administrator the Same Rights as I Have:** Select this option if you want to assign the new administrator the same rights that you have as the currently-logged in administrator.

**4** When you have finished filling in the fields, click *OK* to add the new administrator.

You can also use the `admin-create` command in `zman` to create an administrator account. For more information, see "[Administrator Commands](#)" in the *ZENworks 11 SP2 Command Line Utilities Reference*.

## 6.1.2 Deleting Administrators

- 1 In ZENworks Control Center, click the *Configuration* tab.
- 2 In the Administrators panel, select the check box next to the administrator's name, then click *Delete*.

You can also use the `admin-delete` command in `zman` to delete an administrator account. For more information, see "[Administrator Commands](#)" in the *ZENworks 11 SP2 Command Line Utilities Reference*.

## 6.1.3 Renaming Administrators

You cannot rename an administrator who is created based on an existing user in the user source.

- 1 In ZENworks Control Center, click the *Configuration* tab.
- 2 In the Administrators panel, select the check box next to the administrator's name, click *Edit*, then click *Rename*.
- 3 Specify the new name, then click *OK*.


You can also use the `admin-rename` command in `zman` to rename an administrator account. For more information, see "[Administrator Commands](#)" in the *ZENworks 11 SP2 Command Line Utilities Reference*.

## 6.1.4 Changing Administrator Passwords


To change the password for any administrator account other than the default Administrator account:

- 1 In ZENworks Control Center, click the *Configuration* tab.
- 2 In the Administrators panel, select the check box next to the administrator, click *Edit*, then click *Set Password* to display the Change Administrator Password Dialog box.
- 3 Fill in the fields, then click *OK*.  
Ensure that the password is at least six characters long.

To change the password for the currently logged-in administrator:

- 1 In ZENworks Control Center, click the  icon located next to the *Logout* option in the top right corner.  
The Change Administrator Password dialog box is displayed.
- 2 Fill in the fields, then click *OK*.

To change the password for the default Administrator account:

- 1 Log in using the Administrator account.
- 2 Click the  icon located next to the *Logout* option in the top right corner.  
The Change Administrator Password dialog box is displayed.
- 3 Fill in the fields, then click *OK*.

## 6.2 Managing Administrator Rights

The following sections help you manage existing administrator accounts and their assigned rights:

- ♦ [Section 6.2.1, "Assigning Super Administrator Rights," on page 26](#)
- ♦ [Section 6.2.2, "Assigning Additional Rights," on page 27](#)
- ♦ [Section 6.2.3, "Modifying Assigned Rights," on page 27](#)
- ♦ [Section 6.2.4, "Removing Assigned Rights," on page 28](#)

### 6.2.1 Assigning Super Administrator Rights

A Super Administrator has all rights to perform all actions in ZENworks Control Center. For more information about all of the rights that a Super Administrator has, see [Section 6.5, "Rights Descriptions," on page 32](#). If you grant an administrator Super Administrator rights, any assigned rights that have been allowed, denied, or not set are overridden.

- 1 In ZENworks Control Center, click the *Configuration* tab.
- 2 In the Administrators panel, click the administrator's name.
- 3 Click the *Rights* tab.
- 4 In the General panel, select the *Super Administrator* check box.
- 5 Click *Apply*.

## 6.2.2 Assigning Additional Rights

- 1 In ZENworks Control Center, click the *Configuration* tab.
- 2 Click the administrator in the *Name* column of the Administrators panel.
- 3 Click the *Rights* tab.
- 4 In the Assigned Rights panel, click *Add*, then select the rights you want to assign.
- 5 Fill in the fields.  
For more information, see [Section 6.5, “Rights Descriptions,”](#) on page 32.
- 6 Click *OK*.

You can also use the `admin-rights-set` command in `zman` to assign additional rights for an administrator account. For more information, see “[Administrator Commands](#)” in the [ZENworks 11 SP2 Command Line Utilities Reference](#).

## 6.2.3 Modifying Assigned Rights

- 1 In ZENworks Control Center, click the *Configuration* tab.
- 2 Click the administrator in the *Name* column of the Administrators panel.
- 3 In the Assigned Rights panel, select the check box next to the assigned right.
- 4 Click *Edit*, then modify the settings.  
For more information, see [Section 6.5, “Rights Descriptions,”](#) on page 32.
- 5 Click *OK*.

### Modifying Inventory Report Rights

- 1 In ZENworks Control Center, click the *Configuration* tab.
- 2 Click the administrator in the *Name* column of the Administrators panel.
- 3 Click the *Rights* tab.
- 4 In the Administrator Tasks panel, click *Inventory Report Rights*.
- 5 Select the check box corresponding to the Folder Name for which you want to modify the rights.
- 6 Click *Edit*, then select the rights you want to assign.  
For more information, see [Section 6.5.22, “Inventory Report Rights,”](#) on page 45.

### Modifying Asset Management Report Rights

- 1 In ZENworks Control Center, click the *Configuration* tab.
- 2 Click the administrator in the *Name* column of the Administrators panel.
- 3 Click the *Rights* tab.
- 4 In the Administrator Tasks panel, click *Asset Management Report Rights*.
- 5 Select the check box corresponding to the Folder Name for which you want to modify the rights.
- 6 Click *Edit*, then select the rights you want to assign.  
For more information, see [Section 6.5.23, “Asset Management Report Rights,”](#) on page 45.

## 6.2.4 Removing Assigned Rights

- 1 In ZENworks Control Center, click the *Configuration* tab.
- 2 Click the administrator in the *Name* column of the Administrators pane.
- 3 Select the check box next to the assigned right.
- 4 Click *Delete*.

You can also use the `admin-rights-delete` command in `zman` to delete assigned rights for an administrator account. For more information, see “[Administrator Commands](#)” in the [ZENworks 11 SP2 Command Line Utilities Reference](#).

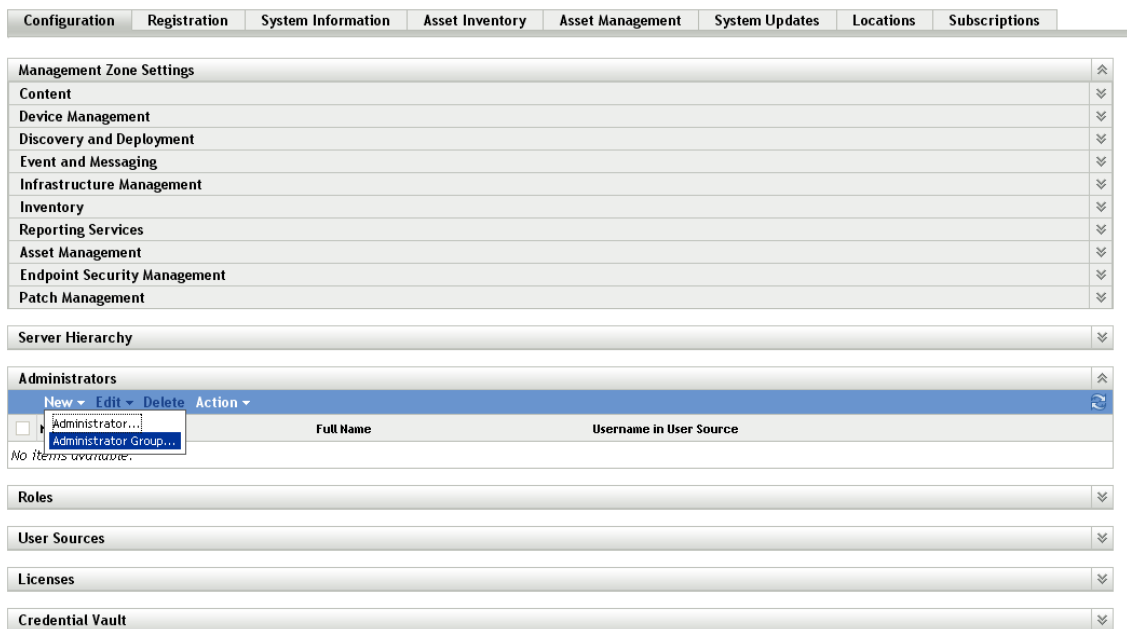
## 6.3 Managing Administrator Group Accounts

The following sections help you create and manage administrator group accounts:

- ♦ [Section 6.3.1, “Creating Administrator Group Account,”](#) on page 28
- ♦ [Section 6.3.2, “Creating Administrators,”](#) on page 30
- ♦ [Section 6.3.3, “Deleting Administrator Groups,”](#) on page 30
- ♦ [Section 6.3.4, “Renaming Administrator Groups,”](#) on page 31

### 6.3.1 Creating Administrator Group Account

- 1 In ZENworks Control Center, click the *Configuration* tab.



- 2 In the Administrators panel, click *New > Administrator Group* to display the Add New Administrator Group dialog box.

Create a new Administrator Group in one of the following ways:

Create a new Administrator Group providing name, description, and members.

Administrator Group Name:

Description:

Add	Remove
<input type="checkbox"/>	<b>Name</b> <span style="float: right;"><b>In Folder</b></span>
<i>No items selected, click add to select items</i>	

Based on user group(s) in a user source will use the same credential defined in Authoritative source.

Add	Remove
<input type="checkbox"/>	<b>Name</b> <span style="float: right;"><b>In Folder</b></span>
<i>No items selected, click add to select items</i>	

Import user members of each user group as administrators immediately.

Fields marked with an asterisk are required.

**3** Fill in the fields.

The Add New Administrator Group dialog box lets you create a new administrator group account by providing a group name and adding members to the group, or you can create a new administrator group based on an existing user group in the user source. Each administrator group name must be unique.

**Create a New Administrator Group by Providing a Name and Adding Members:** Select this option if you want to create a new administrator group account by manually specifying the name and adding the members. To add members, click *Add*, then browse for and select the administrators you want.

You can add any number of administrators to the group. You cannot add other administrator groups to the group.

**Based on User Groups in a User Source:** Select this option if you want to create a new administrator group account based on user group information from your user source. To do so, click *Add*, then browse for and select the user group you want.

**Import user members of each user group as administrators immediately:** Select this option to enable the user members of the selected user groups to be immediately added as administrators who can only view the ZENworks Control Center pages.

- 4 When you have finished filling in the fields, click *OK* to add the new administrator group to the Administrators panel.
- 5 If you need to change the new administrator group's rights or roles, click the administrator group account and then the *Rights* tab to display the account details:

gp1

Summary Rights

Assigned Rights

Add Edit Delete

<input type="checkbox"/>	Type	Context	Allow	Deny
No items available.				

Note: Every admin receives view rights and they are not removable.

Assigned Roles

Add Edit Delete

<input type="checkbox"/>	Role	Type	Context
No items available.			

Apply Reset

- 6 Using the Assigned Rights panel, modify the assigned rights.  
For information about the options on the page, click the *Help* button, or see [“Managing Administrator Group Rights” on page 31](#).
- 7 Using the Assigned Roles panel, modify the assigned roles.  
For information about the options on the page, click the *Help* button, or see [Section 6.6, “Managing Administrator Roles,” on page 46](#).
- 8 When you have finished modifying the rights, click *Apply* to save the changes.

## 6.3.2 Creating Administrators

You can create an administrator account for every user in the administrator group that is created based on an existing user group in the user source.

- 1 In ZENworks Control Center, click the *Configuration* tab.
- 2 In the Administrators panel, select the check box next to the administrator group's name that is created based on an existing user group in the user source.
- 3 Click *Action > Create Administrators*.
- 4 Review the message, then click *OK*

## 6.3.3 Deleting Administrator Groups

- 1 In ZENworks Control Center, click the *Configuration* tab.
- 2 In the Administrators panel, select the check box next to the administrator group's name, then click *Delete*.

## 6.3.4 Renaming Administrator Groups

You cannot rename an administrator group that is created based on an existing user groups in the user source.

- 1 In ZENworks Control Center, click the *Configuration* tab.
- 2 In the Administrators panel, select the check box next to the administrator group's name, click *Edit*, then click *Rename*.
- 3 Specify the new name, then click *OK*.

## 6.4 Managing Administrator Group Rights

The following sections help you manage existing administrator accounts and their assigned rights:

- ♦ [Section 6.4.1, "Assigning Additional Rights," on page 31](#)
- ♦ [Section 6.4.2, "Modifying Assigned Rights," on page 31](#)
- ♦ [Section 6.4.3, "Removing Assigned Rights," on page 31](#)

### 6.4.1 Assigning Additional Rights

- 1 In ZENworks Control Center, click the *Configuration* tab.
- 2 Click the administrator group in the *Name* column of the Administrators panel.
- 3 Click the *Rights* tab.
- 4 In the Assigned Rights panel, click *Add*, then select the rights you want to assign.
- 5 Fill in the fields.  
For more information, see [Section 6.5, "Rights Descriptions," on page 32](#).
- 6 Click *OK*.

### 6.4.2 Modifying Assigned Rights

- 1 In ZENworks Control Center, click the *Configuration* tab.
- 2 Click the administrator group in the *Name* column of the Administrators panel.
- 3 In the Assigned Rights panel, select the check box next to the assigned right.
- 4 Click *Edit*, then modify the settings.  
For more information, see [Section 6.5, "Rights Descriptions," on page 32](#).
- 5 Click *OK*.

### 6.4.3 Removing Assigned Rights

- 1 In ZENworks Control Center, click the *Configuration* tab.
- 2 Click the administrator group in the *Name* column of the Administrators pane.
- 3 Select the check box next to the assigned right.
- 4 Click *Delete*.

## 6.5 Rights Descriptions

When you create additional administrator accounts you can provide full access to your zone or you can create accounts with limited rights. For example, you could create an administrator account that enables the administrator to assign bundles to devices but doesn't allow the administrator to create bundles, or you could create an administrator account that allows access to all management tasks except those pertaining to Management Zone configuration (user sources, registration, configuration settings, and so forth). For information about creating additional administrators, see [“Creating Administrators” on page 24](#).

For [Administrator roles](#) only, a third column of rights options is added to each rights assignment dialog box: *Unset*, which allows rights set elsewhere in ZENworks to be used for the role.

The most restrictive right set in ZENworks prevails. Therefore, if you select the *Deny* option, the right is denied for any administrator assigned to that role, even if the administrator is granted that right elsewhere in ZENworks.

If you select the *Allow* option and the right has not been denied elsewhere in ZENworks, the administrator has that right for the role.

If you select the *Unset* option, the administrator is not granted the right for the role unless it is granted elsewhere in ZENworks.

You can also add, modify, or remove the assigned rights for an existing administrator. For more information, see [Section 6.2.2, “Assigning Additional Rights,” on page 27](#), [Section 6.2.3, “Modifying Assigned Rights,” on page 27](#), or [Section 6.2.4, “Removing Assigned Rights,” on page 28](#).

The following sections contain additional information about the various rights that you can assign:

- ◆ [Section 6.5.1, “Administrator Rights,” on page 33](#)
- ◆ [Section 6.5.2, “Bundle Rights,” on page 33](#)
- ◆ [Section 6.5.3, “Contract Management Rights,” on page 34](#)
- ◆ [Section 6.5.4, “Credential Rights,” on page 34](#)
- ◆ [Section 6.5.5, “Deployment Rights,” on page 35](#)
- ◆ [Section 6.5.6, “Device Rights,” on page 35](#)
- ◆ [Section 6.5.7, “Discovery Rights,” on page 36](#)
- ◆ [Section 6.5.8, “Document Rights,” on page 36](#)
- ◆ [Section 6.5.9, “Inventoried Device Rights,” on page 37](#)
- ◆ [Section 6.5.10, “LDAP Import Rights,” on page 38](#)
- ◆ [Section 6.5.11, “License Management Rights,” on page 38](#)
- ◆ [Section 6.5.12, “Location Rights,” on page 38](#)
- ◆ [Section 6.5.13, “Patch Management Rights,” on page 38](#)
- ◆ [Section 6.5.14, “Policy Rights,” on page 39](#)
- ◆ [Section 6.5.15, “Quick Task Rights,” on page 40](#)
- ◆ [Section 6.5.16, “Remote Management Rights,” on page 41](#)
- ◆ [Section 6.5.17, “Reporting Rights,” on page 42](#)
- ◆ [Section 6.5.18, “Subscription Rights,” on page 42](#)
- ◆ [Section 6.5.19, “User Rights,” on page 42](#)
- ◆ [Section 6.5.20, “ZENworks User Group Rights,” on page 43](#)



- ♦ [Section 6.5.21, “Zone Rights,” on page 43](#)
- ♦ [Section 6.5.22, “Inventory Report Rights,” on page 45](#)
- ♦ [Section 6.5.23, “Asset Management Report Rights,” on page 45](#)

## 6.5.1 Administrator Rights

The Administrator Rights dialog box lets you allow the selected administrator to grant rights to other administrators and to create or delete administrator accounts for your Management Zone.

The following rights are available:

- ♦ **Grant Rights:** Allow or deny the administrator the rights necessary to grant rights to other administrators.
- ♦ **Create/Delete:** Allow or deny the administrator the rights necessary to create or delete administrator accounts.
- ♦ **Create/Delete Groups:** Allow or deny the administrator the rights necessary to create or delete administrator group accounts.
- ♦ **Modify Groups:** Allow or deny the administrator the rights necessary to modify administrator group accounts.

To grant any object rights to other administrators, an administrator must have the *Grant Rights* and the rights for that object. For example, to grant bundle rights to other administrators, an administrator must have both the *Grant Rights* and the *Bundle Rights*.

## 6.5.2 Bundle Rights

The Bundle Rights dialog box lets you select folders containing bundles, then modify the rights associated with those folders.

- ♦ [“Contexts” on page 33](#)
- ♦ [“Privileges” on page 33](#)

### Contexts

To select the folder that contains the bundles for which you want to assign rights, click *Add* to display the Contexts dialog box, then browse for and select the folders for which you want to assign rights.

### Privileges

The *Privileges* section lets you grant the selected administrator rights to create or modify bundles, groups, and folders listed in the [Contexts](#) section.

The following rights are available:

- ♦ **Modify Groups:** Allow or deny the administrator the rights necessary to modify the name or the description of the bundle groups.
- ♦ **Create/Delete Groups:** Allow or deny the administrator the rights necessary to create or delete groups.
- ♦ **Modify Group Membership:** Allow or deny the administrator the rights necessary to modify the list of bundles contained in bundle groups.
- ♦ **Modify Folders:** Allow or deny the administrator the rights necessary to modify folders.

- ♦ **Create/Delete Folders:** Allow or deny the administrator the rights necessary to create or delete folders.
- ♦ **Author:** Allow or deny the administrator the rights necessary to perform changes on bundles, which can be then tested in a testing environment.
- ♦ **Publish:** Allow or deny the administrator the rights necessary to publish tested changes into the production environment. If you assign the publish rights, the author rights also gets assigned by default.
- ♦ **Modify Settings:** Allow or deny the administrator the rights necessary to modify settings.

---

**NOTE:** If you have the Publish rights, then you must also have the Modify Settings right to edit the bundle details such as the bundle’s description, ZENworks Explorer Folder Path, system requirements, and publish a bundle that has existing assignments to a new version. For more information on this, see the trouble shooting scenarios in the “[Troubleshooting](#)” chapter of the [ZENworks 11 SP2 Software Distribution Reference](#).

---

- ♦ **Assign Bundles:** Allow or deny the administrator the rights necessary to assign bundles to the devices or users.

### 6.5.3 Contract Management Rights

The Contract Management Rights dialog box lets you select folders containing contracts, then modify the rights associated with contracts and folders.

- ♦ “[Contexts](#)” on page 34
- ♦ “[Privileges](#)” on page 34

#### Contexts

To select the folder that contains the contracts for which you want to assign rights, click *Add* to display the Contexts dialog box, then browse for and select the folders for which you want to assign rights.

#### Privileges

The *Privileges* section lets you grant the selected administrator rights to contracts and folders listed in the [Contexts](#) section.

- ♦ **Modify:** Allow or deny the administrator the rights necessary to modify the contracts.
- ♦ **Create/Delete:** Allow or deny the administrator the rights necessary to create or delete contracts.
- ♦ **Modify Folder:** Allow or deny the administrator the rights necessary to modify folders.
- ♦ **Create/Delete Folders:** Allow or deny the administrator the rights necessary to create or delete folders.

### 6.5.4 Credential Rights

The Credential Rights dialog box lets you select folders containing credentials, then modify the rights associated with those folders.

- ♦ “[Contexts](#)” on page 35
- ♦ “[Privileges](#)” on page 35

## Contexts

Click *Add* to select the folder that contains the credentials for which you want to assign rights.

## Privileges

The Privileges section lets you grant the selected administrator rights to create or modify credentials, groups, and folders listed in the [Contexts](#) section.

The following rights are available:

- ♦ **Modify:** Allow or deny the administrator the rights necessary to modify credentials.
- ♦ **Create/Delete:** Allow or deny the administrator the rights necessary to create or delete credentials.
- ♦ **Modify Folders:** Allow or deny the administrator the rights necessary to modify folders.
- ♦ **Create/Delete Folders:** Allow or deny the administrator the rights necessary to create or delete folders.

For more information about the tasks you can perform on credentials, see [Chapter 10, “Using the Credential Vault,”](#) on page 87.

### 6.5.5 Deployment Rights

The Deployment Rights dialog box lets you allow or deny the administrator the rights necessary to perform deployment operations.

Deployment lets you discover network devices and deploy the ZENworks Adaptive Agent to them so that they become managed devices in your Management Zone. For more information, see [“ZENworks Adaptive Agent Deployment”](#) in the [ZENworks 11 SP2 Discovery, Deployment, and Retirement Reference](#).

### 6.5.6 Device Rights

The Device Rights dialog box lets you select folders containing devices, then modify the rights associated with those folders.

- ♦ [“Contexts”](#) on page 35
- ♦ [“Privileges”](#) on page 35

## Contexts

To select the folder that contains the devices for which you want to assign rights, click *Add* to display the Contexts dialog box, then browse for and select the folders for which you want to assign rights.

## Privileges

The *Privileges* section lets you grant the selected administrator rights to work with devices, including device groups and folders listed in the [Contexts](#) section.

The following rights are available:

- ♦ **Modify:** Allow or deny the administrator the rights necessary to modify the device objects.

- ♦ **Create/Delete:** Allow or deny the administrator the rights necessary to create or delete device objects.
- ♦ **Modify Groups:** Allow or deny the administrator the rights necessary to modify groups.
- ♦ **Create/Delete Groups:** Allow or deny the administrator the rights necessary to create or delete groups.
- ♦ **Modify Group Membership:** Allow or deny the administrator the rights necessary to modify the list of devices contained in device groups.
- ♦ **Modify Folder:** Allow or deny the administrator the rights necessary to modify folders.
- ♦ **Create/Delete Folders:** Allow or deny the administrator the rights necessary to create or delete folders.
- ♦ **Modify Settings:** Allow or deny the administrator the rights necessary to modify device settings.
- ♦ **Assign Bundles:** Allow or deny the administrator the rights necessary to assign bundles to devices.
- ♦ **Assign Policies:** Allow or deny the administrator the rights necessary to assign policies to devices.
- ♦ **View Detailed Inventory:** Allow or deny the administrator the rights necessary to view the Detailed Hardware/Software Inventory report. Users can edit the detailed summary report only if the modify setting is enabled.
- ♦ **Manage ERI:** Allow or deny the administrator the rights necessary to manage the Emergency Recovery Information (ERI) for device objects. This includes downloading ERI files to use with an Emergency Recovery Disk, viewing ERI file passwords, and deleting ERI files.

## 6.5.7 Discovery Rights

The Discovery Rights dialog box lets you allow or deny the administrator the rights necessary to perform discovery operations.

The following rights are available:

- ♦ **Discovery:** Allow or deny the administrator the right necessary to perform discovery.
- ♦ **Edit Discovered Device:** Allow or deny the administrator the rights necessary to edit a discovered device.

## 6.5.8 Document Rights

The Document Rights dialog box lets you select folders containing documents, then modify the rights associated with documents and folders.

- ♦ [“Contexts” on page 36](#)
- ♦ [“Privileges” on page 37](#)

### Contexts

To select the folder that contains the documents for which you want to assign rights, click *Add* to display the Contexts dialog box, then browse for and select the folders for which you want to assign rights.

## Privileges

The *Privileges* section lets you grant the selected administrator rights to create or modify documents and their folders listed in the [Contexts](#) section.

- ♦ **Modify:** Allow or deny the administrator the rights necessary to reassign documents.
- ♦ **Create/Delete:** Allow or deny the administrator the rights necessary to import or delete documents.
- ♦ **Modify Folder:** Allow or deny the administrator the rights necessary to modify folders.
- ♦ **Create/Delete Folders:** Allow or deny the administrator the rights necessary to create or delete folders.

### 6.5.9 Inventoried Device Rights

The Inventoried Device Rights dialog box lets you select folders containing devices, then modify the rights associated with those folders.

- ♦ [“Contexts” on page 37](#)
- ♦ [“Privileges” on page 37](#)

## Contexts

To select the folder that contains the inventoried devices for which you want to assign rights, click *Add* to display the Contexts dialog box, then browse for and select the folders for which you want to assign rights.

## Privileges

The *Privileges* section lets you grant the selected administrator rights to work with inventoried devices, including device groups and folders listed in the [Contexts](#) section.

The following rights are available:

- ♦ **Modify:** Allow or deny the administrator the rights necessary to modify inventoried device objects.
- ♦ **Create/Delete:** Allow or deny the administrator the rights necessary to create or delete inventoried device objects.
- ♦ **Modify Groups:** Allow or deny the administrator the rights necessary to modify device groups.
- ♦ **Create/Delete Groups:** Allow or deny the administrator the rights necessary to create or delete device groups.
- ♦ **Modify Group Membership:** Allow or deny the administrator the rights necessary to modify the list of devices contained in device groups.
- ♦ **Modify Folder:** Allow or deny the administrator the rights necessary to modify folders.
- ♦ **Create/Delete Folders:** Allow or deny the administrator the rights necessary to create or delete folders.
- ♦ **Modify Settings:** Allow or deny the administrator the rights necessary to modify inventoried device settings.
- ♦ **View Detailed Inventory:** Allow or deny the administrator the rights necessary to view the Detailed Hardware/Software Inventory report. Users can edit the detailed summary report only if the modify setting is enabled.

## 6.5.10 LDAP Import Rights

The LDAP Import Rights dialog box lets you allow or deny importing of LDAP information.

## 6.5.11 License Management Rights

The License Management Rights dialog box lets you select folders containing licenses, then modify the rights associated with licenses and folders.

- ♦ [“Contexts” on page 38](#)
- ♦ [“Privileges” on page 38](#)

### Contexts

To select the folder that contains the licenses for which you want to assign rights, click *Add* to display the Contexts dialog box, then browse for and select the folders for which you want to assign rights.

### Privileges

The Privileges section lets you grant the administrator rights to work with the software license components associated with the contexts (folders) you selected in the [Contexts](#) section

- ♦ **Modify:** Allow or deny the administrator the rights necessary to modify the licenses.
- ♦ **Create/Delete:** Allow or deny the administrator the rights necessary to create or delete licenses.
- ♦ **Modify Folder:** Allow or deny the administrator the rights necessary to modify folders.
- ♦ **Create/Delete Folders:** Allow or deny the administrator the rights necessary to create or delete folders.

## 6.5.12 Location Rights

The Location Rights dialog box lets you modify rights associated with locations in your Management zone. The following rights are available:

- ♦ **Modify:** Allow or deny the administrator the rights necessary to modify the locations
- ♦ **Create/Delete:** Allow or deny the administrator the rights necessary to create or delete locations.

## 6.5.13 Patch Management Rights

The Patch Management Rights dialog box lets you determine which patch management functions an administrator can have.

The following rights are available:

- ♦ **Patch Deploy:** Allow or deny the administrator the rights necessary to deploy patches.
- ♦ **Patch Enable:** Allow or deny the administrator the rights necessary to enable a disabled patch.
- ♦ **Patch Disable:** Allow or deny the administrator the rights necessary to disable a patch.
- ♦ **Patch Update Cache:** Allow or deny the administrator the rights necessary to cache patches.
- ♦ **Assign to Baseline:** Allow or deny the administrator the rights necessary to assign a patch to the baseline.

- ♦ **Remove from Baseline:** Allow or deny the administrator the rights necessary to remove a patch that was assigned to the baseline.
- ♦ **View Patch Details:** Allow or deny the administrator the rights necessary to view patch details.
- ♦ **Export Patch:** Allow or deny the administrator the rights necessary to export patches.
- ♦ **Scan Now:** Allow or deny the administrator the rights necessary to start a scan.
- ♦ **Remove Patch:** Allow or deny the administrator the rights necessary to remove a patch.
- ♦ **Recalculate Baseline:** Allow or deny the administrator the rights necessary to recalculate the baseline.
- ♦ **Configure:** Allow or deny the administrator the rights necessary to configure the patch.

## 6.5.14 Policy Rights

The Policy Rights dialog box lets you select folders containing policies, then modify the rights associated with those folders.

- ♦ [“Contexts” on page 39](#)
- ♦ [“Privileges” on page 39](#)

### Contexts

To select the folder that contains the policies for which you want to assign rights, click *Add* to display the Contexts dialog box, then browse for and select the folders for which you want to assign rights.

### Privileges

The Privileges section lets you grant the selected administrator rights to work with policies, including policy groups and folders listed in the [Contexts](#) section

The following rights are available:

- ♦ **Modify Groups:** Allow or deny the administrator the rights necessary to modify policy groups.
- ♦ **Create/Delete Groups:** Allow or deny the administrator the rights necessary to create or delete policy groups.
- ♦ **Modify Group Membership:** Allow or deny the administrator the rights necessary to modify the list of policies contained in policy groups.
- ♦ **Modify Folders:** Allow or deny the administrator the rights necessary to modify folders.
- ♦ **Create/Delete Folders:** Allow or deny the administrator the rights necessary to create or delete folders.
- ♦ **Author:** Allow or deny the administrator the rights necessary to create, modify, and delete policies. If you enable this right, you must also specify the type of policies (Configuration policies, Security polices, or both) that the administrator can author by enabling the *Manage Configuration Policies* right and/or the *Manage Security Policies* right.
- ♦ **Publish:** Allow or deny the administrator the rights necessary to publish policies. If you enable this right, you must also specify the type of policies (Configuration policies, Security polices, or both) that the administrator can publish by enabling the *Manage Configuration Policies* right and/or the *Manage Security Policies* right.

- ♦ **Assign Policies:** Allow or deny the administrator the rights necessary to assign policies to the devices or users. If you enable this right, you must also specify the type of policies (Configuration policies, Security policies, or both) that the administrator can assign by enabling the *Manage Configuration Policies* right and/or the *Manage Security Policies* right.
- ♦ **Manage Configuration Policies:** Apply the *Author*, *Publish*, and *Assign Policies* rights to Configuration policies. For example, to create, delete, and modify Configuration policies, both the *Author* right and this right must be enabled. To publish Configuration policies, both the *Publish* right and this right must be enabled. To assign Configuration policies, both the *Assign Policies* right and this right must be enabled.

Configuration policies are provided by ZENworks Configuration Management and include the Windows Configuration policies (Browser Bookmarks policy, Dynamic Local User policy, Local File Rights policy, Printer policy, Remote Management policy, Roaming Profile policy, SNMP policy, Windows Group policy, and ZENworks Explorer Configuration policy) and the Linux Configuration policies (External Services policy and Puppet policy).

- ♦ **Manage Security Policies:** Apply the *Author*, *Publish*, and *Assign Policies* rights to Security policies. For example, to create, delete, and modify Security policies, both the *Author* right and this right must be enabled. To publish Security policies, both the *Publish* right and this right must be enabled. To assign Security policies, both the *Assign Policies* right and this right must be enabled.

Security policies are provided by ZENworks Endpoint Security Management (Application Control policy, Communication Hardware policy, Data Encryption policy, Firewall policy, Location Assignment policy, Scripting policy, Security Settings policy, Storage Device Control policy, USB Connectivity policy, VPN Enforcement policy, and Wi-Fi policy) and ZENworks Full Disk Encryption (Full Disk Encryption policy).

## 6.5.15 Quick Task Rights

The Quick Tasks Rights dialog box lets you select folders containing devices, then modify the Quick Task rights associated with those folders.

Quick Tasks are tasks that appear in ZENworks Control Center task lists (for example, Server Tasks, Workstation Tasks, Bundles Tasks, and so forth). When you click a task, either a wizard launches to step you through the task or a dialog box appears in which you enter information to complete the task.

You can use the Quick Tasks Rights dialog box to allow or deny the selected administrator the rights to perform certain tasks by using Quick Tasks.

- ♦ [“Contexts” on page 40](#)
- ♦ [“Privileges” on page 41](#)

### Contexts

To select the folder that contains the device for which you want to assign rights, click *Add* to display the Contexts dialog box, then browse for and select the folders for which you want to assign rights.



## Privileges

The *Privileges* section lets you grant the administrator rights to modify the Quick Task rights associated with the contexts (folders) you selected in the [Contexts](#) section.

The following rights are available:

- ♦ **Shutdown/Reboot/Wake Up Devices:** Specify whether the administrator can shut down, reboot, or wake up the devices in the folders you selected in the list.
- ♦ **Execute Processes:** Allow or deny the administrator the rights necessary to execute processes on the devices.
- ♦ **Refresh ZENworks Adaptive Agent:** Allow or deny the administrator the rights necessary to refresh the ZENworks Adaptive Agent on devices.
- ♦ **Install/Launch Bundles:** Allow or deny the administrator the rights necessary to install or launch bundles. The administrator must also have Assign Bundles rights for devices to install or launch bundles using Quick Task options.
- ♦ **Manage Endpoint Security Settings and Tasks:** Allow or deny the administrator the rights necessary to use Quick Tasks to clear the user-defined encryption password, the local client self defense setting, and the local firewall registration setting. Clearing the local client self defense and firewall registration settings overrides any local changes and reinstates the policy settings.
- ♦ **Inventory:** Allow or deny the administrator the rights necessary to inventory devices.
- ♦ **Apply Image:** Allow or deny the administrator the rights necessary to apply an image to devices.
- ♦ **Take Image:** Allow or deny the administrator the rights necessary to take an image of a device.

## 6.5.16 Remote Management Rights

The Remote Management Rights dialog box lets you select folders containing devices and users, then modify the Remote Management rights associated with those folders. Granting Remote Execute rights allows the administrator to execute processes in the system space.

- ♦ [“Contexts” on page 41](#)
- ♦ [“Privileges” on page 41](#)

## Contexts

To select the folder that contains the devices and users for which you want to assign rights, click *Add* to display the Contexts dialog box, then browse for and select the folders for which you want to assign rights.

## Privileges

The Privileges section lets you grant the administrator rights to modify the Remote Management rights associated with the contexts (folders) you selected in the [Contexts](#) section.

The following rights are available:

- ♦ **Remote Control:** Allow or deny the administrator the rights necessary to remotely control devices.
- ♦ **Remote View:** Allow or deny the administrator the rights necessary to remotely view devices.

- ♦ **Transfer files:** Allow or deny the administrator the rights necessary to transfer files to or from devices.
- ♦ **Remote Execute:** Allow or deny the administrator the rights necessary to remotely execute processes on devices.
- ♦ **Remote Diagnostics:** Allow or deny the administrator the rights necessary to perform remote diagnostic procedures on devices.
- ♦ **Unblock Remote Management Service:** Allow or deny the administrator the rights necessary to unblock the Remote Management Service.

## 6.5.17 Reporting Rights

The Reporting Rights dialog box lets you select folders containing reports, then allows or denies you the rights to create, delete, execute, or publish reports.

- ♦ [“Contexts” on page 42](#)
- ♦ [“Privileges” on page 42](#)

### Contexts

To select the folder that contains the reports for which you want to assign rights, click *Add* to display the Contexts dialog box, then browse for and select the folders for which you want to assign rights.

### Privileges

The Privileges section lets you grant the administrator rights to work with reports associated with the contexts (folders) you selected in the [Contexts](#) section.

- ♦ **Execute/Publish Report Right:** Allows the administrator to schedule reports and manage historical report instances. This right does not allow administrators to create or delete reports or folders within the folder to which the right is assigned. However, the administrator can copy the reports from one folder to another if the destination folder is assigned the Create/Delete Reports right.
- ♦ **Create/Delete Report Right:** Includes the Execute/Publish Report right. It allows the administrators to create, modify, or delete Web Intelligence documents and folders within the folder to which the right is conferred.

## 6.5.18 Subscription Rights

The Subscription Rights dialog box lets you allow or deny the administrator the rights to create and delete subscriptions.

## 6.5.19 User Rights

The User Rights dialog box lets you select folders containing users, then modify the rights associated with those folders.

- ♦ [“Contexts” on page 43](#)
- ♦ [“Privileges” on page 43](#)

## Contexts

To select the folder that contains the users for which you want to assign rights, click *Add* to display the Contexts dialog box, then browse for and select the folders for which you want to assign rights.

## Privileges

The Privileges section lets you grant the selected administrator rights to work with users and folders listed in the [Contexts](#) section.

The following rights are available:

- ♦ **Modify:** Allow or deny the administrator the rights necessary to modify a user object. For example, set a user as a test or non-test user.
- ♦ **Modify ZENworks Group Membership:** Allow or deny the rights necessary to modify ZENworks group membership. If you select this option, you must also grant rights to *Modify ZENworks Group Membership* under *ZENworks User Group Rights*.
- ♦ **Assign Policies:** Allow or deny the administrator the rights necessary to assign policies to users.
- ♦ **Assign Bundles:** Allow or deny the administrator the rights necessary to assign bundles to users.

### 6.5.20 ZENworks User Group Rights

The ZENworks User Group Rights dialog box lets you allow or deny the administrator the rights to create, delete, or modify groups and to modify group membership.

The following rights are available:

- ♦ **Modify Groups:** Allow or deny the administrator the rights necessary to modify existing user groups.
- ♦ **Create/Delete Groups:** Allow or deny the administrator the rights necessary to create or delete user groups.
- ♦ **Modify ZENworks Group Membership:** Allow or deny the administrator the rights necessary to modify the ZENworks group membership. If you select this option, you must also grant rights to *Modify ZENworks Group Membership* under *User Rights*.
- ♦ **Assign Policies:** Allow or deny the administrator the rights necessary to modify the list of policies contained in policy groups.
- ♦ **Assign Bundles:** Allow or deny the administrator the rights necessary to modify the list of bundles contained in policy groups.

### 6.5.21 Zone Rights

The Zone Rights dialog box lets you modify the administrator's rights to administer settings in your ZENworks Management Zone.

The following rights are available:

- ♦ **Modify User Sources:** Allow or deny the administrator the rights necessary to modify user sources.

A user source is an LDAP directory that contains users that you want to reference in your ZENworks Management Zone. When you define a user source, you also define the source containers from which you want to read users and user groups.

Modifying user sources includes adding, removing, or renaming user sources and assigning policies or bundles to user sources.

- ♦ **Create/Delete User Sources:** Allow or deny the administrator the rights necessary to create or delete user sources.
- ♦ **Modify Settings:** Allow or deny the administrator the rights necessary to modify your Management Zone settings.

The Management Zone settings let you manage the global configuration settings for your Management Zone. These global configuration settings are inherited by other objects (devices, users, and folders) within your Management Zone and remain in effect unless they are overridden on those objects.

- ♦ **Modify Zone Infrastructure:** Allow or deny the administrator the rights necessary to modify Zone infrastructure. This right includes the rights to perform the following actions in the Server Hierarchy section of the *Configuration* tab:
  - ♦ Specify content for a device
  - ♦ Move the device in the hierarchy
  - ♦ Configure a Satellite
  - ♦ Add a Satellite
  - ♦ Remove a Satellite

Other actions can be taken in the Server Hierarchy section. However, rights for those actions must be specified individually. They are not automatically included in the Modify Zone Infrastructure right. These are:

- ♦ [Delete ZENworks Server](#)
- ♦ [Refresh Device](#)
- ♦ **Configure Registration:** Allow or deny the administrator the rights necessary to configure device registration.

Registration lets you manage the various configuration settings for registering devices as managed devices in the Management Zone. It also lets you create registration keys or registration rules to help you register devices. A registration key lets you apply group and folder assignments to devices as they register. A registration rule lets you apply group and folder assignments to folders if the device meets the rule criteria.

- ♦ **Create/Delete Local Products:** Allow or deny the administrator the rights necessary to create or delete local software products in the ZENworks Knowledgebase used for asset inventory.
- ♦ **Manage FDE PBA Override:** Allow or deny the administrator the rights necessary to use the Pre-Boot Authentication Override tool (*Full Disk Encryption > Pre-Boot Authentication Override*). The Pre-Boot Authentication Override tool generates challenge/response data that a user can enter during the PBA login to override the PBA and access the device's encrypted drives (for example, in the case of a forgotten password).
- ♦ **Delete News Alerts:** Allow or deny the administrator the rights necessary to delete the news alerts.
- ♦ **Update News Alerts:** Allow or deny the administrator the rights necessary to update the news alerts.

## 6.5.22 Inventory Report Rights

The Inventory Report Rights panel allows you to manage each administrator's rights for each folder and its reports.

Each report folder has rights associated with it, governing all the reports within that folder. For example, if you have full rights, you can edit a report; but with view/execute rights, you can only see the report and run it. With inventory report rights, you can limit who has access to certain reports and who can edit them. The report folder type, custom or standard, and the report name are listed along with the rights associated with the folder. The choices are *Remove All Rights*, *Assign View/Execute Rights*, and *Assign Full Rights*.

### Available Tasks

You can perform the following tasks:

Task	Steps	Additional Details
Remove all rights	<ol style="list-style-type: none"><li>1. Select the report folder.</li><li>2. Click <i>Edit &gt; Remove All Rights</i>.</li></ol>	This removes all rights to the folder, so the specified administrator cannot see it.
Assign view/execute rights	<ol style="list-style-type: none"><li>1. Select the report folder.</li><li>2. Click <i>Edit &gt; Assign View/Execute Rights</i>.</li></ol>	This allows the specified administrator to view and execute a report in the specified folder, but not to edit, move, or delete a report in that folder.
Assign full rights	<ol style="list-style-type: none"><li>1. Select the report folder.</li><li>2. Click <i>Edit &gt; Assign Full Rights</i>.</li></ol>	This gives the specified administrator full rights to create, edit, move, and delete reports. For standard reports, this setting is the same as <i>View/Execute</i> , because you cannot alter a standard report.

## 6.5.23 Asset Management Report Rights

The Asset Management Report Rights panel allows you to manage each administrator's rights for each folder and its reports.

Each report folder has rights associated with it, governing all the reports within that folder. For example, if you have full rights, you can edit a report; but with view/execute rights, you can only see the report and run it. With asset management report rights, you can limit who has access to certain reports and who can edit them. The report folder type, custom or standard, and the report name are listed along with the rights associated with the folder. The choices are *Remove All Rights*, *Assign View/Execute Rights*, and *Assign Full Rights*.

### Available Tasks

You can perform the following tasks:

Task	Steps	Additional Details
Remove all rights	<ol style="list-style-type: none"> <li>1. Select the report folder.</li> <li>2. Click <i>Edit &gt; Remove All Rights</i>.</li> </ol>	This removes all rights to the folder, so the specified administrator cannot see it.
Assign view/execute rights	<ol style="list-style-type: none"> <li>1. Select the report folder.</li> <li>2. Click <i>Edit &gt; Assign View/Execute Rights</i>.</li> </ol>	This allows the specified administrator to view and execute a report in the specified folder, but not to edit, move, or delete a report in that folder.
Assign full rights	<ol style="list-style-type: none"> <li>1. Select the report folder.</li> <li>2. Click <i>Edit &gt; Assign Full Rights</i>.</li> </ol>	This gives the specified administrator full rights to create, edit, move, and delete reports. For standard reports, this setting is the same as <i>View/Execute</i> , because you cannot alter a standard report.

## 6.6 Managing Administrator Roles

Perform the following tasks to manage administrator roles in the Management Zone:

- ♦ [Section 6.6.1, “Understanding Administrator Roles,” on page 46](#)
- ♦ [Section 6.6.2, “Creating a Role,” on page 50](#)
- ♦ [Section 6.6.3, “Assigning Roles,” on page 51](#)
- ♦ [Section 6.6.4, “Editing a Role,” on page 55](#)
- ♦ [Section 6.6.5, “Renaming a Role,” on page 58](#)
- ♦ [Section 6.6.6, “Deleting a Role,” on page 58](#)

### 6.6.1 Understanding Administrator Roles

The roles feature allows Super Administrator to specify rights that can be assigned as roles for ZENworks administrators. You can create a specialized role, then assign administrators to that role to allow or deny them the ZENworks Control Center rights that you specify for that role. For example, you could create a Help Desk role with the ZENworks Control Center rights that you want help desk operators to have. You must be logged-in as a Super Administrator to create and manage the roles.

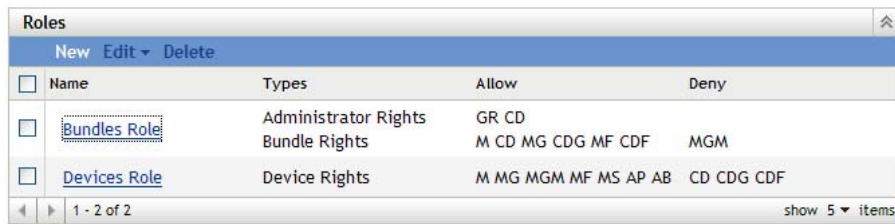
The following sections explain the different locations in ZENworks Control Center where you can manage roles:

- ♦ [“Roles Panel” on page 47](#)
- ♦ [“Role Settings Page” on page 48](#)
- ♦ [“Administrator or Administrator Groups Settings Page” on page 49](#)

## Roles Panel

The Roles panel displays the following information:

**Figure 6-1** Roles Panel



<input type="checkbox"/>	Name	Types	Allow	Deny
<input type="checkbox"/>	<a href="#">Bundles Role</a>	Administrator Rights Bundle Rights	GR CD M CD MG CDG MF CDF	MGM
<input type="checkbox"/>	<a href="#">Devices Role</a>	Device Rights	M MG MGM MF MS AP AB	CD CDG CDF

- ♦ **Name:** You specified this when you created the role. You can rename the role here. You can also click a role name to edit its rights configuration.
- ♦ **Types:** Lists each ZENworks Control Center rights type that is configured for the role.
- ♦ **Allow:** For each type listed, abbreviations are displayed to indicate the rights that are allowed for that role.
- ♦ **Deny:** For each type listed, abbreviations are displayed to indicate the rights that are denied for that role.

If a right is configured as *Unset*, its abbreviation is not listed in either the *Allow* or *Deny* column.

In the Roles panel, you can [add](#), [assign](#), [edit](#), [rename](#), and [delete](#) a role.

## Role Settings Page

If you click a role in the *Name* column on the Roles panel, the Role Settings page is displayed with the following information:

**Figure 6-2** Role Settings Page

[Configuration](#) > Bundles Role

**General** ⌵

Object type: Role

GUID: f4ccf0bcf5b8ab9007540f078572101e

Description:

**Rights** ⌵

Add Edit Delete

<input type="checkbox"/>	Type	Allow	Deny
<input type="checkbox"/>	Administrator Rights	GR CD	
<input type="checkbox"/>	Bundle Rights	M CD MG CDG MF CDF	MGM

1 - 2 of 2 show 5 items

**Assigned Administrators** ⌵

Add Edit Delete

<input type="checkbox"/>	Administrator	Type	Context
<input type="checkbox"/>	<a href="#">Admin1</a>	Administrator Rights Bundle Rights	Zone /Bundles

1 - 1 of 1 show 5 items

- ♦ **General panel:** Displays the ZENworks Control Center object type (Role), its GUID, and a description that you can edit here.
- ♦ **Rights panel:** Displays the ZENworks Control Center rights configured for the role. You can add, edit, and delete the rights in this panel.
- ♦ **Assigned Administrators panel:** Lists the administrators and administrator groups assigned to this role. You can add, edit, or delete the administrators in this panel.



## Administrator or Administrator Groups Settings Page

If you click an administrator in the *Administrator* column on the Roles Settings page and then click the *Rights* tab, the Administrator Settings page is displayed with the following information:

**Figure 6-3** Administrator Settings Page

**General** ⌵

Administrator Full Name:

Super Administrator

Note: If the Super Administrator check box is checked, then this Administrator is a Super Administrator with all rights. This will override any assigned rights that may be allowed, denied, or not set.

**Assigned Rights** ⌵

Add ▾ Edit Delete

<input type="checkbox"/>	Type	Context	Rights
No items available.			

Note: Every admin receives view rights and they are not removable.

**Assigned Roles** ⌵

Add Edit Delete

<input type="checkbox"/>	Role	Type	Context
<input type="checkbox"/>	<a href="#">Bundles Role</a>	Administrator Rights Bundle Rights	Zone /Bundles

show 5 ▾ items

If you click an administrator group in the *Administrator* column on the Roles Settings page and then click the *Rights* tab, the Administrator Settings page is displayed with the following information:

**Figure 6-4** Administrator Groups Settings Page

**Assigned Rights** ⌵

Add ▾ Edit Delete

<input type="checkbox"/>	Type	Context	Rights
No items available.			

Note: Every admin receives view rights and they are not removable.

**Assigned Roles** ⌵

Add Edit Delete

<input type="checkbox"/>	Role	Type	Context
<input type="checkbox"/>	<a href="#">Bundles Role</a>	Administrator Rights Bundle Rights	Zone /Bundles

show 5 ▾ items

- ◆ **General panel:** This panel is not displayed for an administrator group. Displays the administrator's full name and provides the option to specify the administrator as a Super Administrator, which grants all ZENworks Control Center rights to that administrator, regardless of what is configured for the role.
- ◆ **Assigned Rights panel:** Lists the rights that are assigned to the administrator, independent of rights granted or denied by any roles assigned to the administrator. The rights listed in this panel override any rights assigned by a role. You can add, edit, and delete rights in this panel.
- ◆ **Assigned Roles panel:** Lists the roles assigned to this administrator. You can add, edit, and delete roles in this panel.

## 6.6.2 Creating a Role

A role can include one or more rights types. You can configure as many roles as you need. To configure the role's function:

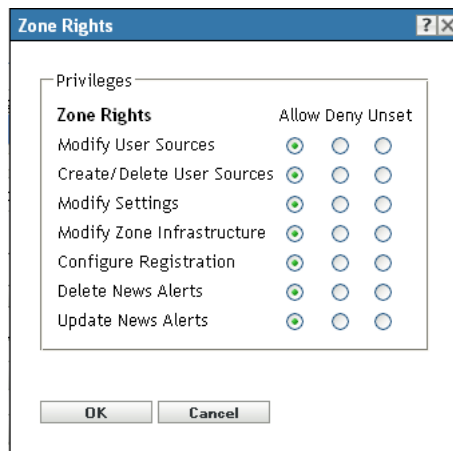
- 1 In ZENworks Control Center, click *Configuration* in the left pane.
- 2 In the Roles panel, click *New* to open the Add New Role dialog box:

The 'Add new Role' dialog box features a 'Name' field with an asterisk, a 'Description' text area, and a 'Rights' section. The 'Rights' section includes 'Add', 'Edit', and 'Delete' buttons, a table with columns 'Type', 'Allow', and 'Deny', and a 'No items available.' message. At the bottom are 'OK' and 'Cancel' buttons.

- 3 Specify a name and description for the role.
- 4 To configure the rights for the role, click *Add* and select a rights type from the drop-down list:

The 'Rights' dialog box shows the 'Add' button dropdown menu open, listing various rights types. The list includes: Administrator Rights, Bundle Rights, Contract Management Rights, Credential Rights, Deployment Rights, Device Rights, Discovery Rights, Document Rights, Inventoried Device Rights, LDAP Import Rights, License Management Rights, Location Rights, Patch Management Rights, Policy Rights, Quick Task Rights, Remote Management Rights, Reporting Rights, Subscriptions Rights, User Rights, ZENworks User Group Rights, and Zone Rights.

- 5 In the following dialog box, select whether each privilege should be allowed, denied, or left unset.



The most restrictive right set in ZENworks prevails. If you select the *Deny* option, the right is denied for any administrator assigned to that role, even if the administrator is granted that right elsewhere in ZENworks.

If you select the *Allow* option and the right has not been denied elsewhere in ZENworks, the administrator has that right for the role.

If you select the *Unset* option, the administrator is not granted the right for the role unless it is granted elsewhere in ZENworks.

- 6 Click *OK* to continue.
- 7 To add another rights type to the role, repeat [Step 4](#) through [Step 6](#).
- 8 Click *OK* to exit the Add New Role dialog box.

The role is now displayed in the Roles panel. To assign it to administrators, see [Section 6.6.3, "Assigning Roles,"](#) on page 51.

### 6.6.3 Assigning Roles

You can assign roles to administrators, or administrators to roles:

- ♦ ["Assigning Roles to Administrators"](#) on page 51
- ♦ ["Assigning Administrators to Roles"](#) on page 53

#### Assigning Roles to Administrators

Rights can be set in multiple locations in ZENworks Control Center, including for administrators. Administrators can be assigned to multiple roles.

If an administrator has rights conflicts because different conditions are set for a particular right in ZENworks Control Center, the *Deny* option is used if it is set anywhere for the administrator. In other words, *Deny* always supersedes *Allow* when there are rights conflicts.

To assign roles to an administrator:

- 1 In ZENworks Control Center, click *Configuration* in the left pane, click the *Configuration* tab, then in the Administrators panel, click an administrator name or an administrator group name in the *Name* column and then click the *Rights* tab to open the administrator's settings page:

**General**

Administrator Full Name:

Super Administrator

Note: If the Super Administrator check box is checked, then this Administrator is a Super Administrator with all rights. This will override any assigned rights that may be allowed, denied, or not set.

---

**Assigned Rights**

Add Edit Delete

<input type="checkbox"/> Type	Context	Rights
No items available.		

Note: Every admin receives view rights and they are not removable.

---

**Assigned Roles**

Add Edit Delete

<input type="checkbox"/> Role	Type	Context
<input type="checkbox"/> <a href="#">Bundles Role</a>	Administrator Rights Bundle Rights	Zone /Bundles

1 - 1 of 1 show 5 items

2 In the Assigned Roles panel, click *Add* to display the Select Role dialog box.

**Select Role**

Select a role

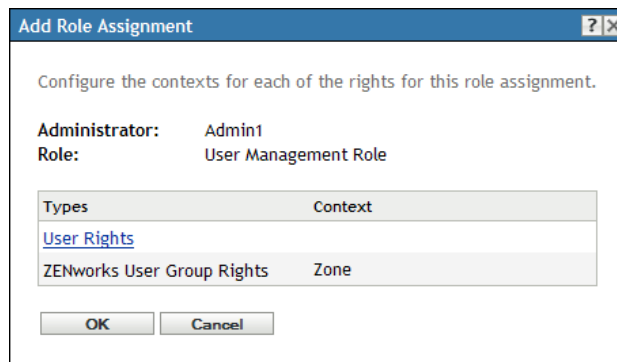
Look in:

Name filter:  Items of type:

Name	Type
<a href="#">Asset Management Role</a>	Role
<a href="#">User Management Role</a>	Role

1 - 2 of 2 show 25 items

- 3 Browse for and select the roles for the administrator, then click *OK* to display the Add Role Assignment dialog box:



The Add Role Assignment dialog box is displayed so that you can define the contexts for the role types included in the role. A context allows you to limit where granted rights can be used. For example, you can specify that the administrator's Quick Task Rights role is limited to the Devices folder in ZENworks Control Center.

Contexts are not required. However, if you do not specify a context, the right is not granted because it has no information about where it can be applied.

Rights that are global automatically display *Zone* as the context.

- 4 If necessary, assign contexts to role types where they are missing:
  - 4a In the *Types* column, click a role type.

Role types that are designated with the *Zone* context are not clickable because they are generally available.
  - 4b In the subsequent Select Context dialog box, click *Add* and browse for a ZENworks Control Center context.

While browsing, you can select multiple contexts in the Browse dialog box.
  - 4c When you are finished selecting the contexts for a particular role, click *OK* to close the Select Contexts dialog box.
  - 4d Repeat [Step 4a](#) through [Step 4c](#) as necessary to assign contexts to the roles.
  - 4e When you are finished, click *OK* to close the Add Role Assignment dialog box.
- 5 To add another administrator, repeat [Step 2](#) and [Step 4](#).
- 6 Click *Apply* to save the changes.

## Assigning Administrators to Roles

Rights can be set in multiple locations in ZENworks Control Center. Administrators can be assigned to multiple roles.

If an administrator has rights conflicts because different conditions are set for a particular right in ZENworks Control Center, the *Deny* option is used if it is set anywhere for the administrator. In other words, *Deny* always supersedes *Allow* when there are rights conflicts.

- 1 In ZENworks Control Center, click *Configuration* in the left pane, click the *Configuration* tab, then in the Roles panel, click a role name in the *Name* column to open the role's settings page:

**General** ⌵

Object type: Role

GUID: f4ccf0bcf5b8ab9007540f078572101e

Description:

**Rights** ⌵

Add ▾ Edit Delete

<input type="checkbox"/>	Type	Allow	Deny
<input type="checkbox"/>	Administrator Rights	GR CD	
<input type="checkbox"/>	Bundle Rights	M CD MG CDG MF CDF	MGM

show 5 ▾ items

**Assigned Administrators** ⌵

Add Edit Delete

<input type="checkbox"/>	Administrator	Type	Context
<input type="checkbox"/>	<a href="#">Admin1</a>	Administrator Rights Bundle Rights	Zone /Bundles

show 5 ▾ items

2 In the Assigned Administrators panel, click *Add* to display the Select Administrator dialog box:

**Select Administrator** ? | X

Select an administrator

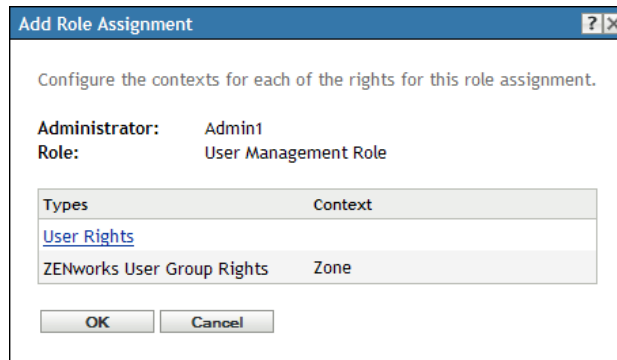
Look in:  ⌵ | 📁

Name filter:  Items of type:  ⌵

	Name	Type
<input type="checkbox"/>	<a href="#">Admin1</a>	Administrator
<input type="checkbox"/>	<a href="#">Admin2</a>	Administrator

show 25 ▾ items

- 3 Browse for and select the administrators or administrator groups for the role, then click *OK* to display the Add Role Assignment dialog box:



The Add Role Assignment dialog box is displayed so that you can define the contexts for the role types included in the role. A context allows you to limit where granted rights can be used. For example, you can specify that the administrator's Quick Task Rights role is limited to the Devices folder in ZENworks Control Center.

Contexts are not required. However, if you do not specify a context, the right is not granted because it has no information about where it can be applied.

Rights that are global automatically display *Zone* as the context.

- 4 If necessary, assign contexts to role types where they are missing:
  - 4a In the *Types* column, click a role type.

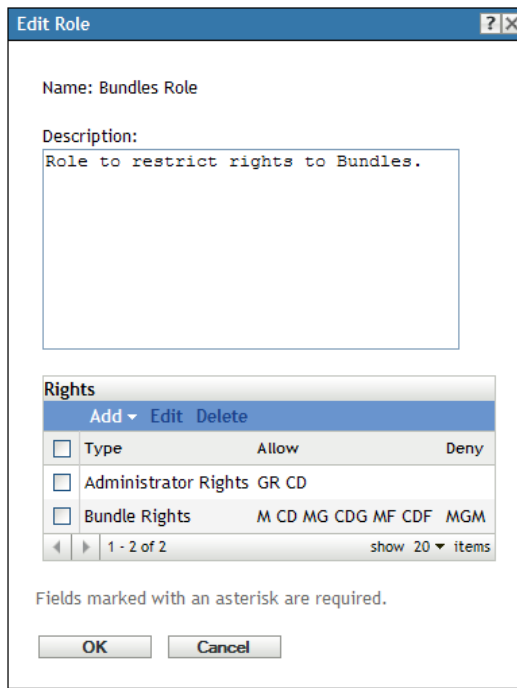
Role types that are designated with the *Zone* context are not clickable because they are generally available.
  - 4b In the subsequent Select Context dialog box, click *Add* and browse for a ZENworks Control Center context.

While browsing, you can select multiple contexts in the Browse dialog box.
  - 4c When you are finished selecting the contexts for a particular role, click *OK* to close the Select Contexts dialog box.
  - 4d Repeat [Step 4a](#) through [Step 4c](#) as necessary to assign contexts to the roles.
  - 4e When you are finished, click *OK* to close the Add Role Assignment dialog box.
- 5 To add another role, repeat [Step 2](#) and [Step 4](#).
- 6 Click *Apply* to save the changes.

## 6.6.4 Editing a Role

You can edit a role's configuration at any time. After you apply the edited role, its changes are then effective for any assigned administrator.

- 1 In ZENworks Control Center, click *Configuration* in the left pane.
- 2 In the Roles panel, select the check box for the role to be edited and click *Edit* to open the Edit Role dialog box:

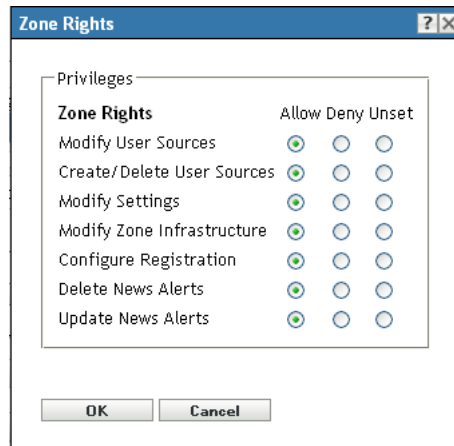


3 To edit the description, make the changes directly in the *Description* field.

4 To edit existing rights, do the following:

4a In the Rights panel, select the check box for a rights type, then click *Edit* to open the Rights dialog box.

For example, select Zone Rights to display the following dialog box:



4b For each privilege, select whether it should be allowed, denied, or left unset.

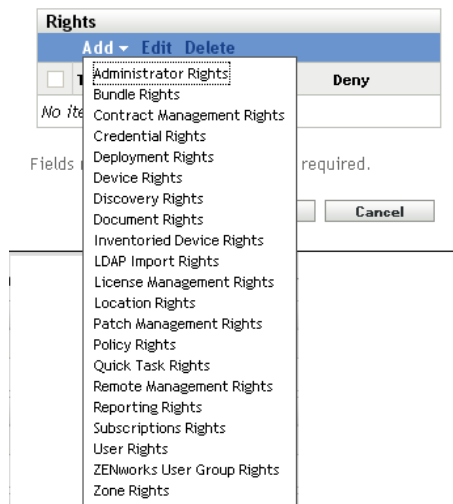
The most restrictive right set in ZENworks prevails. If you select the *Deny* option, the right is denied for any administrator assigned to that role, even if the administrator is granted that right elsewhere in ZENworks.

If you select the *Allow* option and the right has not been denied elsewhere in ZENworks, the administrator has that right for the role.

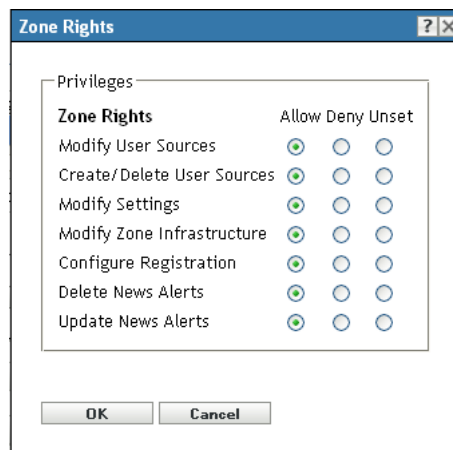
If you select the *Unset* option, the administrator is not granted the right for the role unless it is granted elsewhere in ZENworks.



- 4c Click *OK* to continue.
- 4d To edit another existing role, repeat [Step 4a](#) through [Step 4c](#).
- 5 (Optional) To add new rights:
  - 5a In the Rights panel, click *Add*, then select one of the rights types from the drop-down list:



- 5b In the Rights dialog box, select whether each privilege should be allowed, denied, or left unset.



The most restrictive right set in ZENworks prevails. If you select the *Deny* option, the right is denied for any administrator assigned to that role, even if the administrator is granted that right elsewhere in ZENworks.

If you select the *Allow* option and the right has not been denied elsewhere in ZENworks, the administrator has that right for the role.

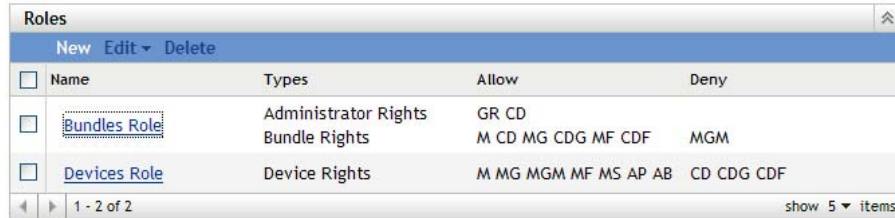
If you select the *Unset* option, the administrator is not granted the right for the role unless it is granted elsewhere in ZENworks.

- 5c Click *OK* to continue.
- 5d To add another rights type to the role, repeat [Step 5a](#) through [Step 5c](#).
- 6 To exit the dialog box and save your changes to the role, click *OK*.

## 6.6.5 Renaming a Role

Role names can be changed at any time. The changed role name is automatically replicated wherever it is displayed in ZENworks Control Center.

- 1 In ZENworks Control Center, click *Configuration* in the left pane.



<input type="checkbox"/>	Name	Types	Allow	Deny
<input type="checkbox"/>	Bundles Role	Administrator Rights Bundle Rights	GR CD M CD MG CDG MF CDF	MGM
<input type="checkbox"/>	Devices Role	Device Rights	M MG MGM MF MS AP AB	CD CDG CDF

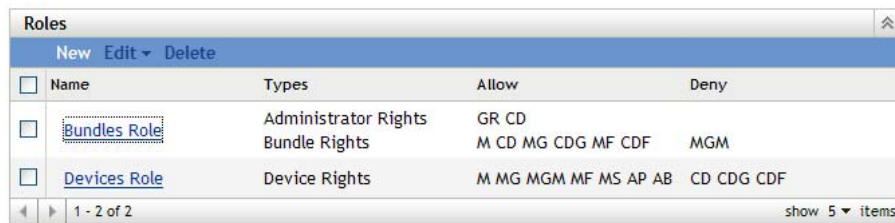
- 2 In the Roles panel, select the check box for the role to be renamed.
- 3 Click *Edit > Rename* to open the Rename Role dialog box:
- 4 Specify the new role name, then click *OK*.

## 6.6.6 Deleting a Role

When you delete a role, its rights configurations are no longer applicable to any administrator that was assigned to the role.

Deleted roles cannot be recovered. You must re-create them.

- 1 In ZENworks Control Center, click *Configuration* in the left pane.
- 2 In the Roles panel, select the check box for the role to be deleted.



<input type="checkbox"/>	Name	Types	Allow	Deny
<input type="checkbox"/>	Bundles Role	Administrator Rights Bundle Rights	GR CD M CD MG CDG MF CDF	MGM
<input type="checkbox"/>	Devices Role	Device Rights	M MG MGM MF MS AP AB	CD CDG CDF

- 3 Click *Delete*, then confirm that you want to delete the role.

---

# 7 Organizing Devices into Folders and Groups

Using ZENworks Control Center, you can manage devices by performing tasks directly on individual device objects. However, this approach is not very efficient unless you have only a few devices to manage. To optimize management of a large number of devices, ZENworks lets you organize devices into folders and groups; you can then perform tasks on a folder or group to manage its devices.

You can create folders and groups at any time. However, the best practice is to create folders and groups before you register devices in your zone. This allows you to use registration keys and rules to automatically add devices to the appropriate folders and groups when they register (see [“Creating Registration Keys and Rules”](#) in the *ZENworks 11 SP2 Discovery, Deployment, and Retirement Reference*).

- ♦ [Section 7.1, “Folders,”](#) on page 59
- ♦ [Section 7.2, “Groups,”](#) on page 61
- ♦ [Section 7.3, “Assignment Inheritance for Folders and Groups,”](#) on page 64

## 7.1 Folders

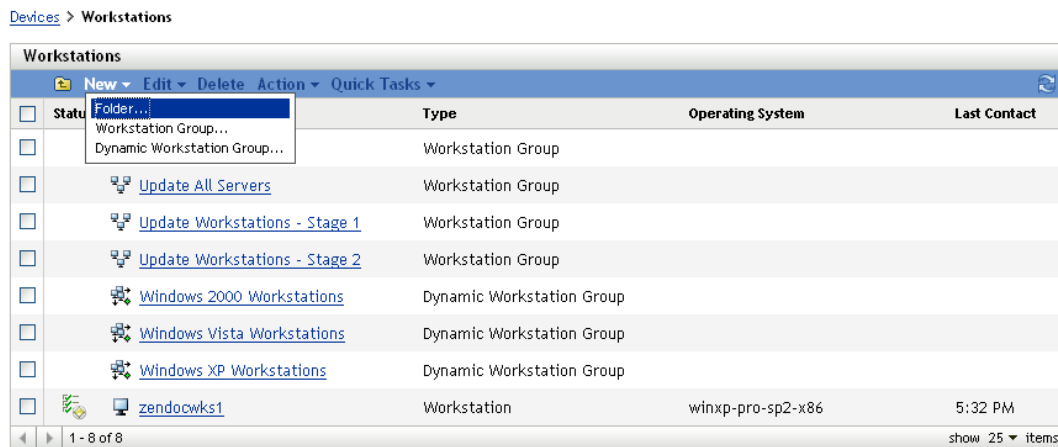
Folders are a great tool to help you organize devices in order to simplify management of those devices. You can apply configuration settings, assign content, and perform tasks on any folder. When you do so, the folder’s devices inherit those settings, assignments, and tasks.

For best results, you should place devices with similar configuration setting requirements in the same folder. If all devices in the folder require the same content or tasks, you can also make content or task assignments on the folder. However, all devices in the folder might not have the same content and task requirements. Therefore, you can organize the devices into groups and assign the appropriate content and tasks to each groups (see [“Groups”](#) on page 61 below).

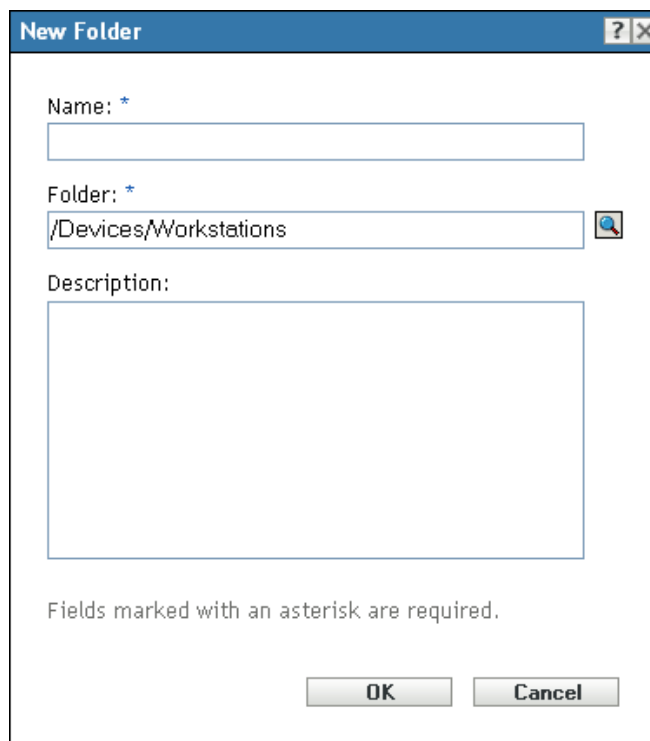
For example, assume that you have workstations at three different sites. You want to apply different configuration settings to the workstations at the three sites, so you create three folders (`/Workstations/Site1`, `/Workstations/Site2`, and `/Workstations/Site3`) and place the appropriate workstations in each folder. You decide that most of the configuration settings apply to all workstations, so you configure those settings at the Management Zone. However, you want to perform a weekly collection of software and hardware inventory at Site1 and Site2 and a monthly inventory collection at Site3. You configure a weekly inventory collection at the Management Zone and then override the setting on the Site3 folder to apply a monthly schedule. Site1 and Site2 collect inventory weekly, and Site3 collects inventory monthly.

## Creating a Folder

- 1 In ZENworks Control Center, click the *Devices* tab.
- 2 Click the *Workstations* folder.



- 3 Click *New > Folder* to display the New Folder dialog box.



- 4 In the *Name* field, type a name for the new folder.  
When you name an object in the ZENworks Control Center (folders, groups, bundles, policies, and so forth), ensure that the name adheres to the following conventions:
  - ◆ The name must be unique in the folder.

- ◆ Depending on the database software being used for the ZENworks database, uppercase and lowercase letters might not create uniqueness for the same name. The embedded database included with ZENworks is case insensitive, so Folder 1 and FOLDER 1 are the same name and cannot be used in the same folder. If you use an external database that is case-sensitive, Folder 1 and FOLDER 1 are unique.
- ◆ If you use spaces, you must enclose the name in quotes when entering it on the command line. For example, you must enclose Folder 1 in quotes ("Folder 1") when entering it in the zman utility.
- ◆ The following characters are invalid and cannot be used: / \ \* ? : " ' < > | ` % ~

5 Click OK to create the folder.

You can also use the `workstation-folder-create` and `server-folder-create` commands in the zman utility to create device folders. For more information, see [“Workstation Commands”](#) and [“Server Commands”](#) in the *ZENworks 11 SP2 Command Line Utilities Reference*.

## 7.2 Groups

As you can with folders, you can also assign content and perform tasks on device groups. When you do so, the group’s devices inherit those assignments and tasks. Unlike with folders, you cannot apply configuration settings to groups.

Groups provide an additional layer of flexibility for content assignments and tasks. In some cases, you might not want to assign the same content to and perform the same task on all devices in a folder. Or, you might want to assign the same content to and perform tasks on one or more devices in different folders. To do so, you can add the devices to a group (regardless of which folders contain the devices) and then assign the content to and perform the tasks on the group.

For example, let’s revisit the example of the workstations at three different sites (see [Section 7.1, “Folders,”](#) on page 59). Assume that some of the workstations at each site need the same accounting software. Because groups can be assigned software, you could create an Accounting group, add the target workstations to the group, and then assign the appropriate accounting software to the group. Likewise, you could use the groups to assign Windows configuration and security policies.

The advantage to making an assignment to a group is that all devices contained in that group receive the assignment, but you only need to make the assignment one time. In addition, a device can belong to any number of unique groups, and the assignments from multiple groups are additive. For example, if you assign a device to group A and B, it inherits the software assigned to both groups.

ZENworks provides both groups and dynamic groups. From the perspective of content assignments or performing tasks, groups and dynamic groups function exactly the same. The only difference between the two types of groups is the way that devices are added to the group. With a group, you must manually add devices. With a dynamic group, you define criteria that a device must meet to be a member of the group, and then devices that meet the criteria are automatically added.

ZENworks include several predefined dynamic server groups (Windows 2000 Servers and Windows 2003 Servers) and dynamic workstation groups (Windows XP Workstation, Windows 2000 Workstation, and Windows Vista Workstations). Any devices that have these operating systems are automatically added to the appropriate dynamic group.

### Creating a Group

- 1 In ZENworks Control Center, click the *Devices* tab.
- 2 If you want to create a group for servers, click the *Servers* folder.

or

If you want to create a group for workstations, click the *Workstations* folder.

[Devices](#) > [Workstations](#)

Workstations					
New ▾ Edit ▾ Delete Action ▾ Quick Tasks ▾					
<input type="checkbox"/>	Status		Type	Operating System	Last Contact
<input type="checkbox"/>		Folder...			
<input type="checkbox"/>		Workstation Group...			
<input type="checkbox"/>		Dynamic Workstation Group...	Workstation Group		
<input type="checkbox"/>		Update All Servers	Workstation Group		
<input type="checkbox"/>		Update Workstations - Stage 1	Workstation Group		
<input type="checkbox"/>		Update Workstations - Stage 2	Workstation Group		
<input type="checkbox"/>		Windows 2000 Workstations	Dynamic Workstation Group		
<input type="checkbox"/>		Windows Vista Workstations	Dynamic Workstation Group		
<input type="checkbox"/>		Windows XP Workstations	Dynamic Workstation Group		
<input type="checkbox"/>		zendocwks1	Workstation	winxp-pro-sp2-x86	5:32 PM

1 - 8 of 8 show 25 items

- 3 Click *New > Server Group* (or *New > Workstation Group* for workstations) to launch the Create New Group Wizard.

[Devices](#) > [Workstations](#) > [Create New Group](#)

**Create New Group**

**Step 1: Basic Information**

Group Name: \*

Folder: \*

Description:

Fields marked with an asterisk are required.

- 4 On the Basic Information page, type a name for the new group in the *Group Name* field, then click *Next*.

The group name must follow the [naming conventions](#).

- 5 On the Summary page, click *Finish* to create the group without adding members.

or

Click *Next* if you want to add members to the group, then continue with [Step 6](#).

- 6 On the Add Group Members page, click *Add* to add devices to the group, then click *Next* when finished adding devices.

- 7 On the Summary page, click *Finish* to create the group.

You can also use the `workstation-group-create` and `server-group-create` commands in the `zman` utility to create device groups. For more information, see “[Workstation Commands](#)” and “[Server Commands](#)” in the *ZENworks 11 SP2 Command Line Utilities Reference*.

## Creating a Dynamic Group

- 1 In ZENworks Control Center, click the *Devices* tab.
- 2 If you want to create a group for servers, click the *Servers* folder.  
or  
If you want to create a group for workstations, click the *Workstations* folder.

[Devices](#) > [Workstations](#)

Workstations				
New ▾ Edit ▾ Delete Action ▾ Quick Tasks ▾				
<input type="checkbox"/>	Status	Type	Operating System	Last Contact
<input type="checkbox"/>	Folder... Workstation Group... Dynamic Workstation Group...	Workstation Group		
<input type="checkbox"/>	Update All Servers	Workstation Group		
<input type="checkbox"/>	Update Workstations - Stage 1	Workstation Group		
<input type="checkbox"/>	Update Workstations - Stage 2	Workstation Group		
<input type="checkbox"/>	Windows 2000 Workstations	Dynamic Workstation Group		
<input type="checkbox"/>	Windows Vista Workstations	Dynamic Workstation Group		
<input type="checkbox"/>	Windows XP Workstations	Dynamic Workstation Group		
<input type="checkbox"/>	zendocwks1	Workstation	winxp-pro-sp2-x86	5:32 PM

1 - 8 of 8 show 25 ▾ items

- 3 Click *New > Dynamic Server Group* (or *New > Dynamic Workstation Group* for workstations) to launch the Create New Group Wizard.

[Devices](#) > [Workstations](#) > [Create New Dynamic Group](#)

**Create New Dynamic Group**

**Step 1: Basic Information**

Group Name: \*

Folder: \*

Description:

Fields marked with an asterisk are required.

---

- 4 On the Basic Information page, type a name for the new group in the *Group Name* field, then click *Next*.

The group name must follow the [naming conventions](#).

- 5 On the Define Filter for Group Members page, define the criteria that a device must meet to become a member of the group, then click *Next*.

Click the *Help* button for details about creating the criteria.

- 6 On the Summary page, click *Finish* to create the group.

## 7.3 Assignment Inheritance for Folders and Groups

This section is applicable only for ZENworks Configuration Management. When you assign content to a folder, all objects (users, devices, subfolders) except groups that are located in the folder inherit the assignment. For example, if you assign BundleA and PolicyB to DeviceFolder1, all devices within the folder (including all devices in subfolders) inherit the two assignments. However, none of the device groups located in DeviceFolder1 inherit the assignments. Essentially, folder assignments do not flow down to groups located within the folder.



---

# 8 Using Message Logging

The Message Logger component of Novell ZENworks 11 SP2 lets the other ZENworks components such as zenloader, web services, ZENworks Management Daemon (ZMD), Remote Management, and Policy Enforcers log messages to different output targets. The output targets includes the system log, local log, database, SMTP, SNMP trap, and UDP.

The following sections provide additional information on the Message Logger component:

- ♦ [Section 8.1, “Functionalities of Message Logger,” on page 65](#)
- ♦ [Section 8.2, “Message Severity,” on page 65](#)
- ♦ [Section 8.3, “Message Format,” on page 66](#)
- ♦ [Section 8.4, “Configuring Message Logger Settings,” on page 66](#)
- ♦ [Section 8.5, “Managing Messages,” on page 70](#)

## 8.1 Functionalities of Message Logger

Message Logger performs the following functions:

- ♦ Writes messages to local log files.
- ♦ Writes messages to a system log or event log.
- ♦ Writes messages to the Management console.
- ♦ Sends messages to the Management server.
- ♦ Sends messages as SMTP mail to SMTP servers from the Primary Server.
- ♦ Sends messages as SNMP traps to remote or local machines from the Primary Server.
- ♦ Sends messages as UDP packets to UDP destinations.
- ♦ Writes messages to the ZENworks database.
- ♦ Automatically purges database entries from the ZENworks database.
- ♦ Automatically acknowledges the messages in the ZENworks database.

## 8.2 Message Severity

A message is an event that is generated by different components and modules. These events can be exceptions such as errors, warnings, information to a user, or a debug statement to debug a module.

Messages are classified based on the following severity levels:

**Error:** Indicates that an action cannot be completed because of a user or system error. These messages are critical and require immediate attention from an administrator.

**Warning:** Indicates an exception condition. These messages might not be an error but can cause problems if not resolved. These messages do not require immediate attention from an administrator.

**Information:** Provides feedback about something that happened in the product or system that is important and informative for an administrator.

**Debug:** Provides debug information to troubleshoot and solve problems that might occur. The debug messages are stored only in the local file.

## 8.3 Message Format

Messages are logged in different formats depending on the output targets. For more information on message formats see, [Section 8.5.1, “Understanding Message Formats,” on page 71.](#)

## 8.4 Configuring Message Logger Settings

The following sections provide information on configuring the settings of the Message Logger component of Novell ZENworks 11 SP2.

- ♦ [Section 8.4.1, “Configuring the Message Logger Settings at the Zone Level,” on page 66](#)
- ♦ [Section 8.4.2, “Configuring the Message Logger Settings at the Folder Level,” on page 69](#)
- ♦ [Section 8.4.3, “Configuring the Message Logger Settings at the Device Level,” on page 70](#)
- ♦ [Section 8.4.4, “Turning on the Debug Messages,” on page 70](#)

### 8.4.1 Configuring the Message Logger Settings at the Zone Level

The following sections contain information to help you configure the settings in the Management Zone to enable message logging:

- ♦ [“Local Device Logging” on page 66](#)
- ♦ [“Centralized Message Logging” on page 67](#)


#### Local Device Logging

In ZENworks Control Center, the Local Device Logging page lets you configure the message logging to a local drive and the system log file of the managed device.

- 1 In ZENworks Control Center, click *Configuration*.
- 2 In the Management Zone Settings panel, click *Device Management*, then click *Local Device Logging*.
- 3 Configure the following options in the Local File panel:

**Log Message to a Local File if Severity Is:** Choose from one of the following:

- ♦ **Error:** Stores messages with a severity of Error.
- ♦ **Warning and Above:** Stores messages with a severity of Warning and Error.
- ♦ **Information and Above:** Stores messages with a severity of Information, Warning, and Error.
- ♦ **Debug and Above:** Stores messages with a severity of Debug, Information, Warning, and Error.

If you need to troubleshoot a ZENworks Adaptive Agent issue on an individual device, you can change the severity setting so that additional information is logged. On the device, double-click the  icon in the notification area, click *Logging* in the left navigation pane, then select an option from the *Log Messages if Severity Is* drop-down list.

**Rolling Based on Size:** Closes the current log file and starts a new file based on the file size:

- ♦ **Limit File Size to:** Specify the maximum size of the log file, in either kilobytes (KB) or megabytes (MB). The log file is closed after the size of the file reaches the specified limit and a new file is started.
- ♦ **Number of Backup Files:** Specify the number of closed files to be backed up. The maximum number of backup files is 13.

**Rolling Based on Date:** Closes the current log file and starts a new file based on the following schedules:

- ♦ **Daily Pattern:** Starts a new file daily.
- ♦ **Monthly Pattern:** Starts a new file monthly.

On a Windows managed device, the local files include the following:

- ♦ `zmd-messages.log` located in `\novell\zenworks\logs\localstore`
- ♦ `loader-messages.log` located in `\novell\zenworks\logs`
- ♦ `services-messages.log` located in `\novell\zenworks\logs`

On a Linux managed device, the local files include the following:

- ♦ `loader-messages.log` located in `/var/opt/novell/log/zenworks`
- ♦ `services-messages.log` located in `/var/opt/novell/log/zenworks`

#### 4 Configure the following options in the System Log panel.

**Send Message to Local System Log and Roll Up to Collection Server if Severity Is:** Allows you to select the severity of the message to be sent to the local system log and rolled up to the Collection Server. Choose from one of the following:

- ♦ **Error:** Stores messages with severity of Error.
- ♦ **Warning and Above:** Stores messages with a severity of Warning and Error.
- ♦ **Information and Above:** Stores messages with a severity of Information, Warning, and Error.

This setting lets you determine the message types that are added to the local system log. The local system log is the `\var\log\messages` directory on Linux devices and the `zenworks/logs/centralstore` directory on Windows devices.

Messages added to this system log directory are sent to the ZENworks Server for viewing in ZENworks Control Center on the *Configuration > System Information* page or by viewing the Summary page for the server or workstation.

## Centralized Message Logging

In ZENworks Control Center, the Centralized Message Logging page lets you configure the settings related to message logging performed by the Primary Server.

- 1 In ZENworks Control Center, click *Configuration*.
- 2 In the Management Zone Settings panel, click *Event and Messaging*, then click *Centralized Message Logging*.
- 3 In the Automatic Message Cleanup panel, configure the settings to automatically acknowledge or remove the logged messages from the ZENworks server:

**Preferred Maintenance Server:** Specify the IP address of the preferred server on which the Message Cleanup actions runs to acknowledge or delete the logged messages from database.

**Information:** Allows you to configure the following settings for the informational messages:

- ♦ **Auto acknowledge when older than [ ] days:** Allows you to automatically acknowledge the logged informational messages that are older than the number of days you specify. For example, if you specify 30 days, then all the informational messages logged before 30 days from the current date are acknowledged when the Message Cleanup activity is scheduled to run. If you specify zero, then the informational messages dated until today are acknowledged. By default, all the informational messages older than 60 days are automatically acknowledged.
- ♦ **Auto delete when older than [ ] days:** Allows you to automatically delete the logged informational messages that are older than the number of days you specify. For example, if you specify 30 days, then all the informational messages logged before 30 days from the current date are deleted when the Message Cleanup activity is scheduled to run. If you specify zero, then the informational messages dated until today are deleted. By default, all the informational messages older than 60 days are automatically deleted.

If you want to specify both the auto-acknowledge and auto-delete days, then the number of auto-acknowledge days should always be less than the number for auto-delete days.

**Warnings:** Allows you to configure the following settings for the warning messages:

- ♦ **Auto acknowledge when older than [ ] days:** Allows you to automatically acknowledge the logged warning messages that are older than the number of days you specify. For example, if you specify 30 days, then all the warning messages logged before 30 days from the current date are acknowledged when the Message Cleanup activity is scheduled to run. If you specify zero, then the warning messages dated until today are acknowledged. By default, all the warning messages older than 60 days are automatically acknowledged.
- ♦ **Auto delete when older than [ ] days:** Allows you to automatically delete the logged warning messages that are older than the number of days you specify. For example, if you specify 30 days, then all the warning messages logged before 30 days from the current date are deleted when the Message Cleanup activity is scheduled to run. If you specify zero, then the warning messages dated until today are deleted. By default, all the warning messages older than 60 days are automatically deleted.

If you want to specify both the auto-acknowledge and auto-delete days, then the number of auto-acknowledge days should always be less than the number for auto-delete days.

**Errors:** Allows you to configure the following settings for the error messages:

- ♦ **Auto acknowledge when older than [ ] days:** Allows you to automatically acknowledge the logged error messages that are older than the number of days you specify. For example, if you specify 30 days, then all the error messages logged before 30 days from the current date are acknowledged when the Message Cleanup activity is scheduled to run. If you specify zero, then the error messages dated until today are acknowledged. By default, all the error messages older than 60 days are automatically acknowledged.
- ♦ **Auto delete when older than [ ] days:** Allows you to automatically delete the logged error messages that are older than the number of days you specify. For example, if you specify 30 days, then all the error messages logged before 30 days from the current date are deleted when the Message Cleanup activity is scheduled to run. If you specify zero, then error messages dated until today are deleted. By default, all the error messages older than 60 days are automatically deleted.

If you want to specify both the auto-acknowledge and auto-delete days, then the number of auto-acknowledge days should always be less than the number for auto-delete days.

**Select the Days of the Week and the Time to Perform the Message Cleanup:** Allows you to specify the time and the days of the week to run the Message Cleanup action. The administrator can set a daily schedule for Message Cleanup action.

**Use Coordinated Universal Time:** Allows you to convert the specified time to UTC (GMT) time. By default, this option is selected.

- 4 In the E-mail Notification panel, configure the settings to send the error messages to the administrators through e-mail:

**Send Log Message via E-mail if Severity Is:** Allows you to select the severity of the message to trigger sending the log messages through e-mail.

**From:** Specify the sender's e-mail address.

**To:** Specify the e-mail address of the recipients. You can specify more than one e-mail address by separating them with commas.

**Subject:** Specify the subject to be included while sending the e-mail from the Primary Server. You can customize the *Subject* field with macro values. For more information on customizing the subject field, see [“E-Mail Format” on page 71](#).

- 5 In the SNMP Traps panel, configure the SNMP traps on the ZENworks Server to send log messages:

**Send as SNMP Trap if Severity Is:** Sends an SNMP trap if the logged message's severity is Error.

**Trap Target:** Specify the IP address or DNS name of the SNMP server.

**Port:** Specify the port number of the SNMP server configured for this operation. By default, the port number is 162.

**Community String:** Specify the community string of the SNMP trap that is to be sent.

- 6 In the UDP Forwarder panel, configure the settings to send logged messages through the UDP services. The following table contains information on the options available:

**Send Message via UDP:** Sends messages to the UDP destinations if the logged message's severity is Error.

**UDP Destinations:** You can perform the following tasks with the *Add*, *Edit*, and *Remove* options:

- ◆ **Add a Server**

1. Click *Add* to display the Add UDP Destination Address dialog box.
2. Specify the server name and the UDP port number configured for this operation.
3. Click *OK*.

- ◆ **Remove a Server**

1. Select the check box next to the server (or servers).
2. Click *Remove*.

- ◆ **Edit Server Details**

1. Select the check box next to the server.
2. Click *Edit* to display the Edit UDP Destination dialog box.
3. Modify the settings as desired, then click *OK*.

## 8.4.2 Configuring the Message Logger Settings at the Folder Level

By default, the Message Logger settings configured at the zone level are applied to all the managed devices. However, you can modify the Local Device Logging settings for all the devices within a folder:

- 1 In ZENworks Control Center, click *Devices*.
- 2 Click the *Folder (Details)* option for which you want to configure the Message Logger settings.

- 3 Click *Settings*, then click *Device Management > Local Device Logging*.
- 4 Click *Override*.
- 5 Edit the logging settings as required.
- 6 To apply the changes, click *Apply*.  
or  
To revert to the Local Device Logging settings configured at the zone level, click *Revert*.
- 7 Click *OK*.

### 8.4.3 Configuring the Message Logger Settings at the Device Level

By default, the Message Logger settings configured at the zone level are applied to all the managed devices. However, you can modify the Local Device Logging settings for the managed device:

- 1 In ZENworks Control Center, click *Devices*.
- 2 Click *Servers* or *Workstations* to display the list of managed devices.
- 3 Click the device for which you want to configure the Message Logger settings.
- 4 Click *Settings*, then click *Device Management > Local Device Logging*.
- 5 Click *Override*.
- 6 Edit the logging settings as required.
- 7 To apply the changes click *Apply*.  
or  
To revert to the Local Device Logging settings configured at the zone level, click *Revert*.
- 8 Click *OK*.

### 8.4.4 Turning on the Debug Messages

To turn on the logging of debug messages for all components:

- 1 In ZENworks Control Center, click *Configuration*.
- 2 In the Management Zone Settings panel, click *Device Management*, then click *Local Device Logging*.
- 3 In the local file panel, select the *Log message to a local file if severity is* option, then select the severity as *Debug and above*.
- 4 Click *Apply*, then click *OK*.

## 8.5 Managing Messages

The Message Logger component lets you manage the messages logged by the other components of Novell ZENworks 11 SP2.

- ♦ [Section 8.5.1, "Understanding Message Formats," on page 71](#)
- ♦ [Section 8.5.2, "Viewing the Message Status," on page 73](#)
- ♦ [Section 8.5.3, "Viewing the Messages," on page 75](#)
- ♦ [Section 8.5.4, "Acknowledging Messages," on page 76](#)
- ♦ [Section 8.5.5, "Deleting Messages," on page 78](#)
- ♦ [Section 8.5.6, "Viewing the Predefined Reports," on page 80](#)

## 8.5.1 Understanding Message Formats

- ♦ “Local Log File Format” on page 71
- ♦ “E-Mail Format” on page 71
- ♦ “SNMP Message Format” on page 72
- ♦ “UDP Payload Format” on page 73

Messages are logged in different formats depending on the output targets such as local log, e-mail notification, SNMP traps, and UDP notification.

All error messages log the component name on which the error is generated. To troubleshoot the error, refer to the component’s Reference Guide.

**Example 1:** Error related to Policy Management.

```
[DEBUG] [7/22/2007 3:42:45 PM] [] [PolicyManager] [] [Name = RM_dev, Guid = 271414163524d000190dbc6fa94272aa, Type = remote management policy, Version = 2] [] []].
```

To troubleshoot this error, see the [ZENworks 11 SP2 Configuration Policies Reference](#).

**Example 2:** Error related to Remote Management.

```
[ERROR] [15-07-2007 12:44:16] [] [Remote Management] [RemoteManagement.VNCEVENT_CANNOT_OPEN_EVENT] [Unable to open the <ZRMUserLoginEvent> event] [] []].
```

To troubleshoot this error, see the [ZENworks 11 SP2 Remote Management Reference](#).

### Local Log File Format

Messages are logged on the managed device and ZENworks Server in the following format:

```
[severity] [loggingTime] [userGUID] [componentName] [MessageID] [MessageString] [additionalInfo] [RelatedGUID].
```

For example, [DEBUG] [1/22/2007 12:09:15 PM] [] [ZMD] [] [refreshing QuickTaskRefresh(GeneralRefresh)] [] []].

### E-Mail Format

An e-mail message consists of the message header and the message body:

- ♦ “Message Header” on page 71
- ♦ “Message Body” on page 72

### Message Header

The subject field in the e-mail can be customized as required by using keyword substitution macros:

Macro	Value
%s	Severity of the message.
%c	Name of the component.
%d	ID of the device at which the message is generated.
%t	Time of the message generation.
%a	Alias name of the device where the message is generated.

For example, if you want the subject line to display as “ERROR occurred on device Testifies at 4/1/07 5:31:01 PM”, then specify “%s occurred on device %a at %t” in the *Subject* field.

## Message Body

The message body consists of the following fields:

- ♦ **Device Alias:** Name of the device where the message is generated.
- ♦ **Device IP Address:** IP Address of the device where the message is generated.
- ♦ **Error:** [Date] Component name Message ID localized message string.
- ♦ **Additional Information:** (Optional) Any additional information.

## SNMP Message Format

The SNMP messages consists of the following two parts:

- ♦ [“SNMP Message Header” on page 72](#)
- ♦ [“Protocol Data Unit \(PDU\)” on page 72](#)

### SNMP Message Header

The following fields are contained in the header:

**Version Number:** Specifies the version of SNMP used. ZENworks 11 uses SNMPv1.

**Community String:** Defines an access environment for a group of network-management systems (NMS).

### Protocol Data Unit (PDU)

The following fields are contained in the PDU:

**Enterprise:** Identifies the type of managed object generating the trap. ZENworks 11 uses 1.3.6.1.4.1.23.2.80.100.

**Agent Address:** Provides the IP address of the machine where the trap was generated.

**Generic Trap Type:** Contains the integer value 6. Type 6 is an enterprise-specific trap type, which has no standard interpretation in SNMP. The interpretation of the trap depends upon the value in the specific trap type field, which is defined by the Message Logger MIB.



**Specific Trap Code:** For enterprise-specific traps generated by ZENworks 11, the values in the specific trap type fields are as follows:

- ◆ For a severity level of MessageLogger.ERROR, the specific trap is 1.
- ◆ For a severity level of MessageLogger.WARN, the specific trap is 2.
- ◆ For a severity level of MessageLogger.INFO, the specific trap is 3.

**Time Stamp:** The time stamp indicating when the trap occurred.

**Variable Bindings:** Provides additional information pertaining to the trap. This field consists of the following name/value pairs:

- ◆ For trap ID 1.3.6.1.4.1.23.2.80.100.0.1, the value is the device GUID.
- ◆ For trap ID 1.3.6.1.4.1.23.2.80.100.0.2, the value is the device name.
- ◆ For trap ID 1.3.6.1.4.1.23.2.80.100.0.3, the value is the component name.
- ◆ For trap ID 1.3.6.1.4.1.23.2.80.100.0.4, the value is the time when the message was logged.
- ◆ For trap ID 1.3.6.1.4.1.23.2.80.100.0.5, the value is the message ID.
- ◆ For trap ID 1.3.6.1.4.1.23.2.80.100.0.6, the value is the probable cause.

## UDP Payload Format

The payload is a byte array with null-terminated delimiters such as `\0` or `0 x 00` (hexadecimal) for each element. Each element's data is presented as UTF-8 encoded strings and is explained below:

- ◆ The first element is the ZENworks version information. For example, 10.
- ◆ The second element is the value of severity of the message. The severity values are 4 for Informational, 6 for Warning, and 8 for Debug messages.
- ◆ The third element is the message date. The date is not locally specific and is represented as a UTF-8 string. For example, 09-Mar-2008 14:15:44.
- ◆ The fourth element is the user ID.
- ◆ The fifth element is the component name.
- ◆ The sixth element is the non-localized message ID.
- ◆ The seventh element is the localized message string.
- ◆ The eighth element is the additional information.
- ◆ The ninth element is the probable cause URL.
- ◆ The tenth element is the related GUID objects separated by commas.

---

**NOTE:** If the element does not have any data, it is represented as `\0\0`.

---

## 8.5.2 Viewing the Message Status

In ZENworks Control Center, you can view the status of the logged messages in the following panels on the home page.

- ◆ [“Message Summary” on page 74](#)
- ◆ [“Device Hot List” on page 74](#)

## Message Summary

The Message Summary panel displays the number of critical, warning, and normal messages generated on the main objects in the Management Zone.

**Figure 8-1** Message Summary

Message Summary				
				Total
Servers	3	0	5	8
Workstations	9	1	1	11
Policies	3	0	17	20
Bundles	2	0	5	7

In the Message Summary panel, you can do the following:

- Click an object type to display its root folder. For example, click *Servers* to display the Servers root folder.
- For any object type, click the number in one of its status columns (, , ) to display a listing of all the objects that currently have that status. For example, to see the list of servers that have a normal status, click the number in the column of the *Servers*.
- For any object type, click the number in the *Total* column to display all of the objects of that type having critical, warning, or normal messages. For example, click the Total count for *Servers* to display a list of all servers having messages logged.

## Device Hot List

The Device Hot List displays a list of the devices that have a noncompliant status or have generated critical or warning messages. The device remains in the hot list until you resolve the compliancy problem and acknowledge the messages. You can use this list as a summary of problems that need attention on the device.



To view the Device Hot List:

- In ZENworks Control Center, click the *Home* tab.

Device Hot List				
			Type	Item
3	45	22		<a href="#">blr-nrm-r6a</a>
2	28	27		<a href="#">blr-nrm-r9a</a>
2	25	23		<a href="#">blr-nrm-r5v2</a>
2	0	0		<a href="#">blr-nrm-r3f</a>
1	52	1		<a href="#">blr-nrm-r11d</a>

1 - 5 of 15 show 5 items

- This column indicates the number of bundles or policies that could not be applied to the device because an error occurred. You must review the error and warning messages to discover the compliance problem. The noncompliant status applies only to ZENworks Configuration Management. ZENworks Asset Management does not use this status.

- ◆  This column indicates the number of unacknowledged error messages generated for the device. An error is any action that fails so the ZENworks Adaptive Agent cannot complete the action on the device.
- ◆  This column indicates the number of unacknowledged warning messages generated for the device. A warning is any action that encounters a problem; the problem might or might not result in the ZENworks Adaptive Agent completing the action on the device.

2 Click the device to display its message log.

### 8.5.3 Viewing the Messages

In the ZENworks Control Center, you can view the logged messages as follows:

- ◆ [“Message Log” on page 75](#)
- ◆ [“System Message Log” on page 76](#)

#### Message Log







The Message Log displays all unacknowledged messages generated for the object.

To view the message logs:

- 1 In ZENworks Control Center, click the *Device Hot List* on the home page, then click the device to view its message log.

You can also use the *Devices* menu to view the logs:


- 1 In ZENworks Control Center, click *Devices*.
- 2 Click *Servers* or *Workstations* to display the list of managed devices.
- 3 Click the name of a device, then click the *Summary* tab to display:

Message Log			Advanced 
Status	Message	Date	
	<a href="#">The action local file rights policy (ID:local file rights policy)</a>	3:20 AM	
	<a href="#">The drive "d:" is not a local fixed drive. Files/folders on this</a>	3:20 AM	
	<a href="#">The action local file rights policy (ID:local file rights policy)</a>	3:14 AM	
	<a href="#">The drive "d:" is not a local fixed drive. Files/folders on this</a>	3:14 AM	
	<a href="#">The action grouppolicy (ID:grouppolicy) failed, but the action s</a>	3:11 AM	

1 - 5 of 91 show 5 items

**Status:** Displays an icon indicating the type of message:

 Critical Message

 Warning

 Normal

**Message:** Displays a brief description of the event that occurred.

**Date:** Displays the date and time the event occurred.

- 4 To view the log messages in the advanced view, click *Advanced* on the right corner of the Memory Log panel.

You can acknowledge or delete messages from the message log. For more information on acknowledging messages, see [Section 8.5.4, “Acknowledging Messages,” on page 76](#), and for information on deleting messages, see [Section 8.5.5, “Deleting Messages,” on page 78](#).

## System Message Log

The System Message Log panel displays the unacknowledged messages generated by the ZENworks Servers and managed devices in the Management Zone.

- 1 In ZENworks Control Center, click *Configuration*.
- 2 Click *System Information* to display the System Message Log.

System Message Log				Advanced
Status	Message	Date	Source	
	POLICYHANDLERS.PrinterPolicy.LocalPrinterAddSuccess(http://164.9	10:24 AM	blr-nrm-r5v2	
	POLICYHANDLERS.PrinterPolicy.LocalPrinterAddSuccess(printerlocal)	10:23 AM	blr-nrm-r5v2	
	Printer \\164.99.154.214\share already exists for user , hence n	10:23 AM	blr-nrm-r5v2	
	The action printer policy (ID:printer policy) failed, but the ac	10:23 AM	blr-nrm-r5v2	
	IPrint client is already installed in the device, not reinstalli	10:23 AM	blr-nrm-r5v2	

1 - 5 of 820 show 5 items

**Status:** Displays an icon indicating the type of message:

- Critical Message
- Warning
- Normal

**Message:** Displays a brief description of the event that occurred.

**Date:** Displays the date and time the event occurred.

- 3 To view the log messages in the advanced view, click *Advanced* on the right corner of the System Memory Log panel.

You can acknowledge or delete messages from the system message log. For more information on acknowledging messages, see [Section 8.5.4, “Acknowledging Messages,” on page 76](#), for information on deleting messages, see [Section 8.5.5, “Deleting Messages,” on page 78](#).

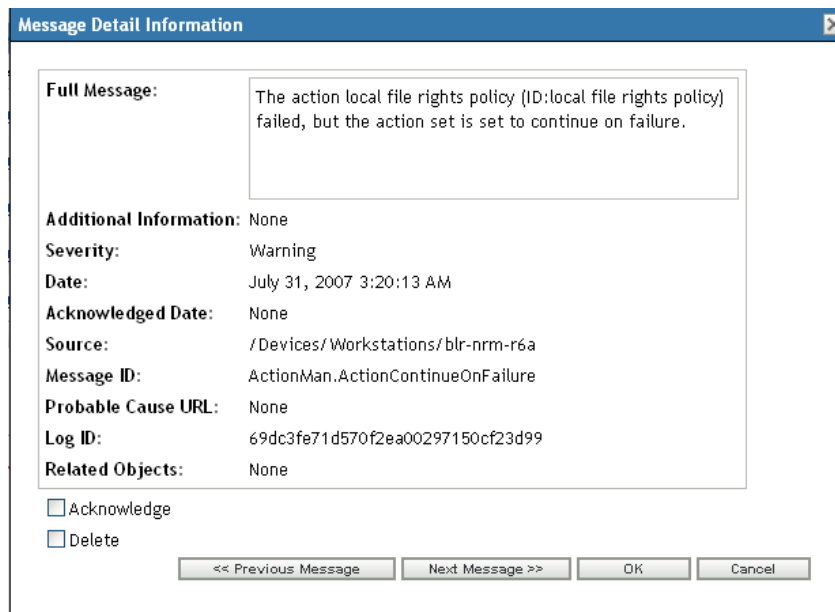
## 8.5.4 Acknowledging Messages

An acknowledged message is one that you have reviewed and marked as acknowledged ()

- ♦ [“Acknowledging a Message” on page 76](#)
- ♦ [“Acknowledging Multiple Messages” on page 77](#)
- ♦ [“Acknowledging Messages Logged During a Specified Time” on page 77](#)

### Acknowledging a Message

- 1 In the Message Log panel or the System Message Log panel, click the message you want to acknowledge.
- 2 In the Message Detail Information dialog box, select the *Acknowledge* option, then click *OK*:



The acknowledged messages are removed from the Message Log panel or the System Message Log panel, depending on which panel you selected in [Step 1](#).

The acknowledged messages continue to be listed in the Advanced view of these logs, marked with a check mark (✓).

## Acknowledging Multiple Messages

- 1 In the Message Log panel or the System Message Log panel, click *Advanced* on the right corner of the panel.
- 2 Select the messages to acknowledge, then click *Acknowledge*:

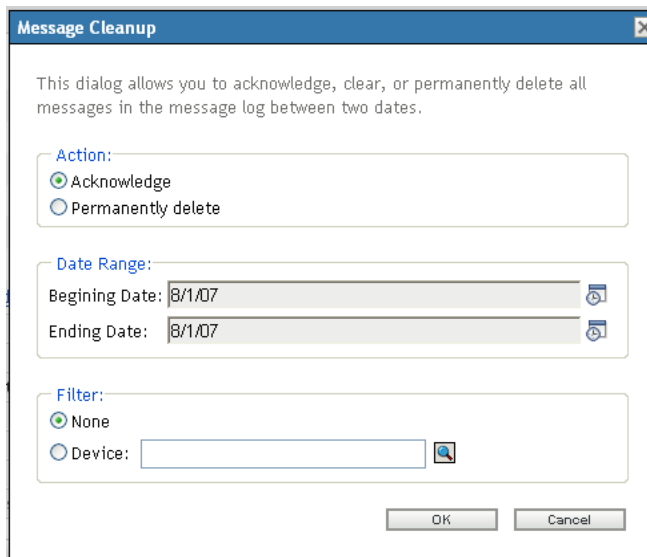
Acknowledge		Delete	
<input type="checkbox"/> Status	Message	Date	✓
<input type="checkbox"/>	<a href="#">The action local file rights policy (ID:local file rights policy)</a>	7/31/07 5:20:32 AM	✓
<input type="checkbox"/>	<a href="#">The drive "d:" is not a local fixed drive. Files/folders on this</a>	7/31/07 5:20:31 AM	✓
<input type="checkbox"/>	<a href="#">The action local file rights policy (ID:local file rights policy)</a>	7/31/07 3:20:13 AM	
<input type="checkbox"/>	<a href="#">The drive "d:" is not a local fixed drive. Files/folders on this</a>	7/31/07 3:20:12 AM	
<input type="checkbox"/>	<a href="#">The action local file rights policy (ID:local file rights policy)</a>	7/31/07 3:14:39 AM	

1 - 5 of 93 show 5 items

The acknowledged messages are marked with a check mark (✓).

## Acknowledging Messages Logged During a Specified Time

- 1 In ZENworks Control Center, click *Configuration*.
- 2 In the *Configuration Tasks*, click *Message Cleanup* to display:



- 3 In the Message Cleanup dialog box, select *Acknowledge*.
- 4 In the *Date Range* option, select the *Beginning Date* and the *Ending Date*.
- 5 Select the *Filter* option:
  - None:** Cleans up the messages in selected date range from all the devices.
  - Device:** Cleans up the messages in selected date range from the selected device.
- 6 Click *OK*.

A message cleanup action is initiated and a system message is logged after the cleanup action is completed. For more information on viewing system logs, see [“System Message Log” on page 76](#).

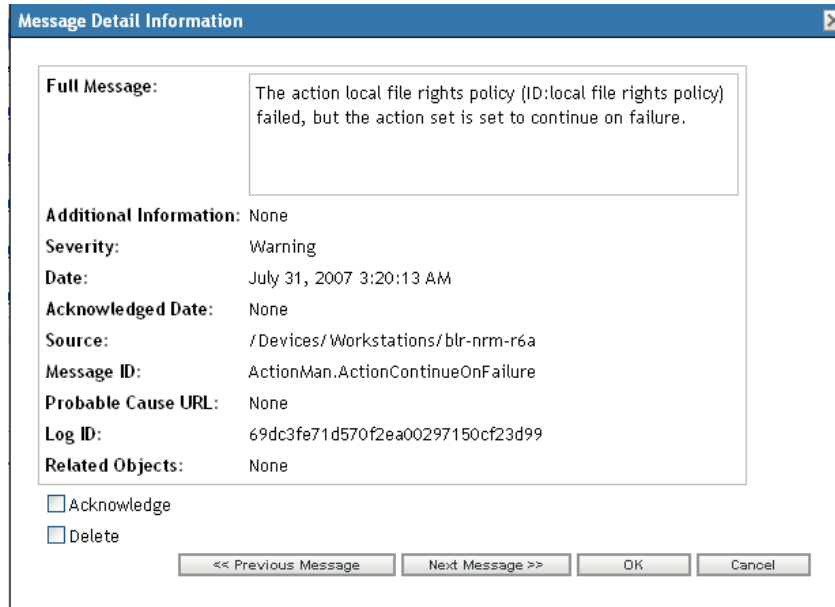
## 8.5.5 Deleting Messages

Deleting a message completely removes the message from your ZENworks system.

- ♦ [“Deleting a Message” on page 79](#)
- ♦ [“Deleting Multiple Messages” on page 79](#)
- ♦ [“Deleting Messages Logged During a Specified Time” on page 79](#)

## Deleting a Message

- 1 In the Message Log panel or the System Message Log panel, click the message you want to delete.
- 2 In the Message Detail Information dialog box, select the *Delete* option, then click *OK*:



## Deleting Multiple Messages

- 1 In the Message Log panel or the System Message Log panel, click *Advanced* on the right corner of the panel.

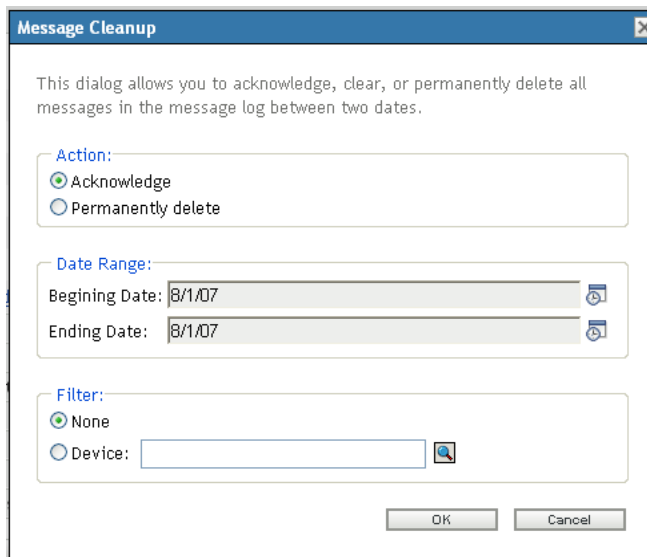
Acknowledge		Delete		
<input type="checkbox"/>	Status	Message	Date	✓
<input type="checkbox"/>	✓	<a href="#">The action local file rights policy (ID:local file rights policy)</a>	7/31/07 5:20:32 AM	✓
<input type="checkbox"/>	✗	<a href="#">The drive "d:" is not a local fixed drive. Files/folders on this</a>	7/31/07 5:20:31 AM	✓
<input type="checkbox"/>	✓	<a href="#">The action local file rights policy (ID:local file rights policy)</a>	7/31/07 3:20:13 AM	
<input type="checkbox"/>	✗	<a href="#">The drive "d:" is not a local fixed drive. Files/folders on this</a>	7/31/07 3:20:12 AM	
<input type="checkbox"/>	✓	<a href="#">The action local file rights policy (ID:local file rights policy)</a>	7/31/07 3:14:39 AM	

1 - 5 of 93 items      show 5 items

- 2 Select the messages to delete, then click *Delete*.

## Deleting Messages Logged During a Specified Time

- 1 In ZENworks Control Center, click *Configuration*.
- 2 In the *Configuration Tasks*, click *Message Cleanup*.



- 3 In the Message Cleanup dialog box, select *Permanently Delete*.
- 4 In the *Date Range* option, select the *Beginning Date* and the *Ending Date*.
- 5 Select the *Filter* option:
  - None:** Cleans up the messages in selected date range from all the devices.
  - Device:** Cleans up the messages in selected date range from the selected device.
- 6 Click *OK*.
- 7 In the Confirm Delete Dialog box, click *OK* to delete the message.

A system message is logged after the cleanup action is completed. For more information on viewing the system log see, "[System Message Log](#)" on page 76.

## 8.5.6 Viewing the Predefined Reports

You must have installed ZENworks Reporting Server to view the predefined reports. For more information on how to install ZENworks Reporting Server, see the [ZENworks 11 Installation Guide](#).

To view the predefined reports for messages:

- 1 In ZENworks Control Center, click the *Reports* tab.
- 2 In the ZENworks Reporting Server Reporting panel, click *ZENworks Reporting Server InfoView* to launch the ZENworks Reporting Server InfoView.
- 3 Navigate to the *Novell ZENworks Reports* folder > *Predefined Reports* > *ZENworks System* folder.
- 4 The following predefined report is included for Messages:
  - ZENworks Messages:** Displays message details such as the log time and description for all the ZENworks System messages.

For more information on creating and managing reports, see the [ZENworks 11 System Reporting Reference](#) documentation.



# 9 Customizing ZENworks News Alerts

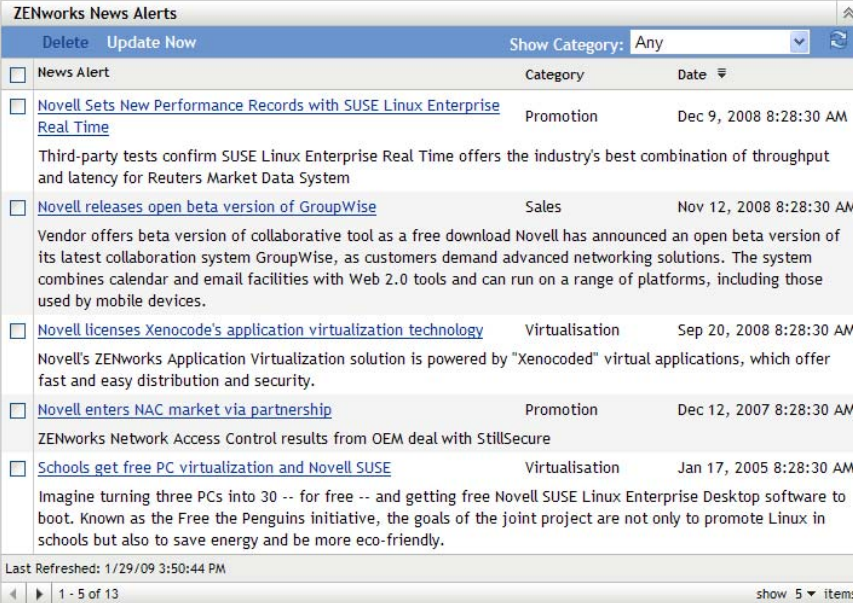
Novell ZENworks 11 SP2 displays information from Novell about current top issues, news updates, promotions, and so forth on the home page of ZENworks Control Center.

The following sections provide information on deleting, updating, and sorting the news alerts, and on viewing the news. You can also configure the server and the schedule for downloading the news.

- ♦ [Section 9.1, “Managing ZENworks News Alerts,”](#) on page 81
- ♦ [Section 9.2, “Configuring ZENworks News Settings,”](#) on page 82

## 9.1 Managing ZENworks News Alerts

*Figure 9-1 ZENworks News Alerts*



<input type="checkbox"/> News Alert	Category	Date
<input type="checkbox"/> <a href="#">Novell Sets New Performance Records with SUSE Linux Enterprise Real Time</a> Third-party tests confirm SUSE Linux Enterprise Real Time offers the industry's best combination of throughput and latency for Reuters Market Data System	Promotion	Dec 9, 2008 8:28:30 AM
<input type="checkbox"/> <a href="#">Novell releases open beta version of GroupWise</a> Vendor offers beta version of collaborative tool as a free download Novell has announced an open beta version of its latest collaboration system GroupWise, as customers demand advanced networking solutions. The system combines calendar and email facilities with Web 2.0 tools and can run on a range of platforms, including those used by mobile devices.	Sales	Nov 12, 2008 8:28:30 AM
<input type="checkbox"/> <a href="#">Novell licenses Xenocode's application virtualization technology</a> Novell's ZENworks Application Virtualization solution is powered by "Xenocoded" virtual applications, which offer fast and easy distribution and security.	Virtualisation	Sep 20, 2008 8:28:30 AM
<input type="checkbox"/> <a href="#">Novell enters NAC market via partnership</a> ZENworks Network Access Control results from OEM deal with StillSecure	Promotion	Dec 12, 2007 8:28:30 AM
<input type="checkbox"/> <a href="#">Schools get free PC virtualization and Novell SUSE</a> Imagine turning three PCs into 30 -- for free -- and getting free Novell SUSE Linux Enterprise Desktop software to boot. Known as the Free the Penguins initiative, the goals of the joint project are not only to promote Linux in schools but also to save energy and be more eco-friendly.	Virtualisation	Jan 17, 2005 8:28:30 AM

Last Refreshed: 1/29/09 3:50:44 PM  
1 - 5 of 13 items

Review the following sections to manage the ZENworks News Alerts:

- ♦ [Section 9.1.1, “Deleting the News Alerts,”](#) on page 82
- ♦ [Section 9.1.2, “Updating the News Alerts,”](#) on page 82
- ♦ [Section 9.1.3, “Displaying the News Alerts Based on the Selected Category,”](#) on page 82
- ♦ [Section 9.1.4, “Viewing the News,”](#) on page 82
- ♦ [Section 9.1.5, “Sorting the News Alerts,”](#) on page 82

## 9.1.1 Deleting the News Alerts

- 1 In ZENworks Control Center, click *Home*.
- 2 In ZENworks News Alerts panel, select the check box next to the news alerts you want to delete.
- 3 Click *Delete*.

## 9.1.2 Updating the News Alerts

- 1 In ZENworks Control Center, click *Home*.
- 2 In ZENworks News Alerts panel, click *Update Now*.  
The latest ZENworks news updates downloaded by the Primary Server are displayed in the ZENworks News Alerts panel. This might take some time.

## 9.1.3 Displaying the News Alerts Based on the Selected Category

- 1 In ZENworks Control Center, click *Home*.
- 2 In ZENworks News Alerts panel, select a category in the drop-down list next to *Show Category* to display all the news alerts based on the selected category.

## 9.1.4 Viewing the News

- 1 In ZENworks Control Center, click *Home*.
- 2 In ZENworks News Alerts panel, click the news alert to display the news in a new browser window.

## 9.1.5 Sorting the News Alerts

By default, the news alerts are sorted by the publication date. You can also sort the news alerts alphabetically by the title or category.

- 1 In ZENworks Control Center, click *Home*.
- 2 In ZENworks News Alerts panel, click *News Alert* to sort the news alerts alphabetically.  
or  
Click *Category* to sort the news alerts by category.  
or  
Click *Date* to sort the news alerts by date.

## 9.2 Configuring ZENworks News Settings

The ZENworks News Settings page lets you configure a dedicated news server and a schedule to download the ZENworks news. By default, the news is downloaded at midnight by the Primary Server of the Management Zone.

**Figure 9-2** News Download Schedule

News Download Schedule

To download news in a restrictive environment, select a server that has access to the Internet through proxy. Otherwise, news is randomly downloaded by a primary server in the zone.

Dedicated News Server:

This setting allows the administrator to configure a download schedule for News.

Schedule Type:

Recurring

Days of the week

Sun	Mon	Tue	Wed	Thu	Fri	Sat
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Start Time: 12:00 am

Hide Options

Process Immediately If device unable to execute on schedule

Use Coordinated Universal Time (Current UTC 5:34 AM)

Start at a random time between Start and End Times

End Time: 1:00 am

Restrict schedule execution to the following date range:

Start Date: 12/17/08

End Date: 12/17/08

Review the following sections to configure the settings to download the news:

- ◆ [Section 9.2.1, “Dedicated News Server,” on page 83](#)
- ◆ [Section 9.2.2, “Schedule Type,” on page 84](#)

## 9.2.1 Dedicated News Server

By default, any available server in the Management Zone can be used to download the news updates. However, you can specify one ZENworks Server to be dedicated to handle the news downloads. The server that you select should have access to the Internet, either directly or through a proxy server.

The following sections contain more information:


- ◆ [“Specifying a Dedicated News Server” on page 83](#)
- ◆ [“Clearing a Dedicated News Server” on page 84](#)

### Specifying a Dedicated News Server

- 1 In ZENworks Control Center, click *Configuration* in the left pane.
- 2 On the *Configuration* tab, expand the *Management Zone Settings* section (if necessary), click *Infrastructure Management*, then click *ZENworks News Settings* to display the News Download Schedule panel.
- 3 In the *Dedicated News Server* field, browse for and select a server, then click *OK*.  
The server’s identification is displayed in the *Dedicated News Server* field.
- 4 (Conditional) If you need to revert to the last saved dedicated server setting, click *Reset*.  
This resets the dedicated server to the last saved setting, such as when you last clicked *Apply* or *OK*.
- 5 Click *Apply* to make the changes effective.
- 6 Either click *OK* to close the page, or continue with configuring the [schedule type](#).  
If you did not click *Apply* to make your changes effective, clicking *OK* does so. Clicking *Cancel* also closes the page, but loses your unapplied changes.

## Clearing a Dedicated News Server

Clearing a dedicated update server causes the news updates to be retrieved randomly from any server in the Management Zone.

- 1 In ZENworks Control Center, click *Configuration* in the left pane.
- 2 On the *Configuration* tab, expand the *Management Zone Settings* section (if necessary), click *Infrastructure Management*, then click *ZENworks News Settings* to display the News Download Schedule panel.
- 3 Click  to remove the dedicated server from the *Dedicated News Server* field.
- 4 (Conditional) If you need to revert to the last saved dedicated server setting, click *Reset*.  
This resets the dedicated server to the last saved setting, such as when you last clicked *Apply* or *OK*.
- 5 Click *Apply* to make the change effective.

### 9.2.2 Schedule Type

You can configure the schedule for downloading the news:

- 1 In ZENworks Control Center, click *Configuration* in the left pane, then click the *Configuration* tab.
- 2 Click *Management Zone Settings* to expand its options, click *Infrastructure Management* to expand its options, then select *ZENworks News Settings*.
- 3 (Conditional) To exclude scheduled checking for news updates, click the down-arrow in the *Schedule Type* field, select *No Schedule*, click *Apply* to save the schedule change, then skip to [Step 6](#).

With this option selected, you must download the news updates manually. For more information, see [“Updating the News Alerts” on page 82](#).

- 4 (Conditional) To set a recurring schedule for checking for the news updates, click the down-arrow in the *Schedule Type* field, then select *Recurring*.
- 5 Fill in the fields:
  - 5a Select one or more check boxes for the days of the week when you want to check for news updates.
  - 5b Use the *Start Time* box to specify the time of day for checking to occur.
  - 5c (Optional) Click *More Options*, then select the following options as necessary:
    - ♦ **Process Immediately if Device Unable to Execute on Schedule:** Causes checking for news updates to occur as soon as possible if the checking cannot be done according to schedule. For example, if a server is down at the scheduled time, checking for news updates occurs immediately after the server comes back online.
    - ♦ **Use Coordinated Universal Time:** Causes the schedule to interpret the times you specify as UTC instead of local time.
    - ♦ **Start at a Random Time Between Start and End Times:** Allows checking for news updates to occur at a random time between the time you specify here and the time you specified in [Step 5b](#). Fill in the *End Time* fields.
    - ♦ **Restrict Schedule Execution to the Following Date Range:** In addition to the other options, you can specify a date range to check for the news updates.
  - 5d (Conditional) If you need to revert to the last saved schedule, click *Reset* at the bottom of the page.

This resets all data to the last saved state, such as when you last clicked *Apply* or *OK*.

- 5e** When you have finished configuring the recurring schedule, click *Apply* to save the schedule change.
  - 6** To exit this page, click *OK* when you are finished configuring the schedule.
- If you did not click *Apply* to make your changes effective, clicking *OK* does so. Clicking *Cancel* also closes the page, but loses your unapplied changes.



# 10 Using the Credential Vault

The Credential Vault stores the credentials used by Novell ZENworks 11 SP2 actions and tasks that require authentication to access a particular resource.

For example, if you want to create a third-party Imaging bundle by using the image files stored in a shared-network image repository that requires authentication, you can add a credential that includes the login name and password for the repository in the credential vault. During the creation of the third-party Imaging bundle, you can specify the credential name to access the repository.

ZENworks features like Third-party imaging, Intel AMT provisioning, Subscriptions download, and actions such as Copy Directory uses credentials that are stored in the credential vault.

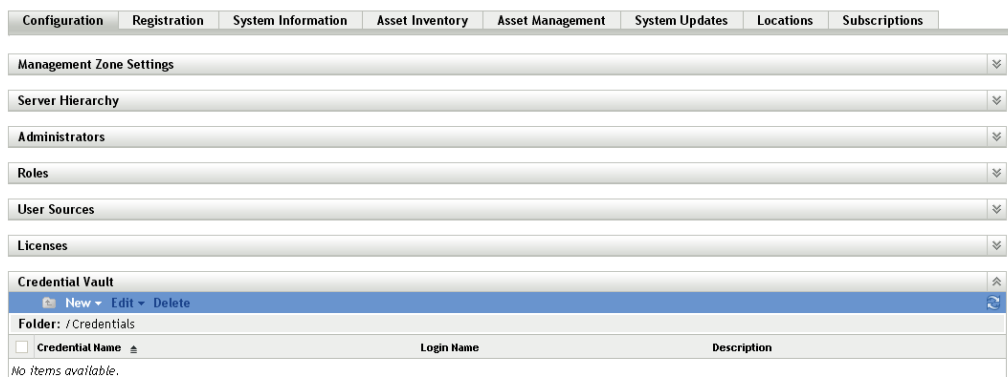
You can use ZENworks Control Center or the zman command line utility to manage credentials. The procedures in this section explain how to manage credentials by using ZENworks Control Center. If you prefer the zman command line utility, see [“Credential Commands”](#) in the *ZENworks 11 SP2 Command Line Utilities Reference*.

The following sections contain information to help you manage credentials:

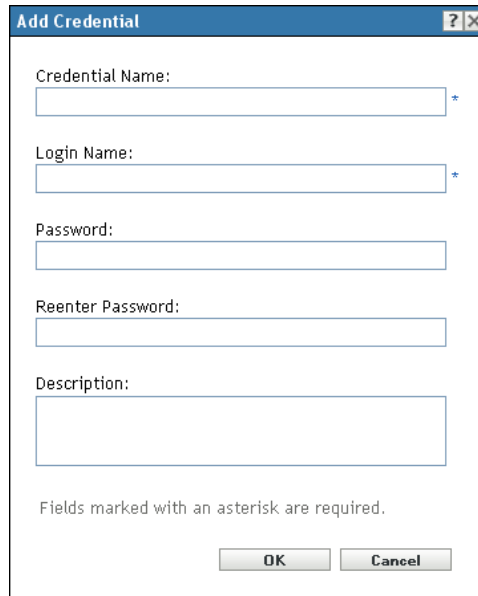
- ◆ [Section 10.1, “Adding a Credential,”](#) on page 87
- ◆ [Section 10.2, “Creating a Folder for Credentials,”](#) on page 89
- ◆ [Section 10.3, “Assigning Credential Rights,”](#) on page 90
- ◆ [Section 10.4, “Editing a Credential,”](#) on page 90
- ◆ [Section 10.5, “Renaming a Credential,”](#) on page 91
- ◆ [Section 10.6, “Moving a Credential to Another Folder,”](#) on page 91
- ◆ [Section 10.7, “Removing a Credential,”](#) on page 91

## 10.1 Adding a Credential

- 1 In ZENworks Control Center, click the *Configuration* tab.



- 2 In the *Credential Vault* panel, click *New > Credential* to display the Add Credential dialog box.



The screenshot shows a dialog box titled "Add Credential". It contains the following fields and labels:

- Credential Name: [text box] \*
- Login Name: [text box] \*
- Password: [text box]
- Reenter Password: [text box]
- Description: [text box]

Fields marked with an asterisk are required.

Buttons: OK, Cancel

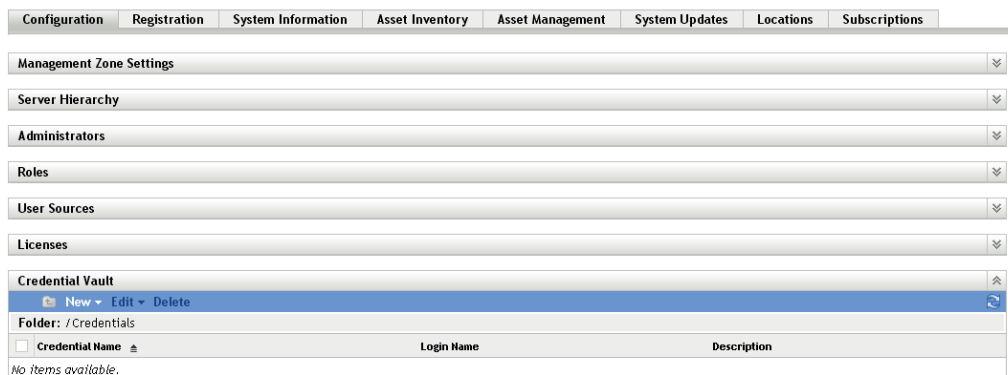
- 3 Fill in the following fields.

- ◆ **Credential Name:** Specify the name of the credential. When an action or task that requires authentication is executed, ZENworks uses this name to access the credential vault to obtain the resource's credentials.
- ◆ **Description:** Provide an optional description of the credential.
- ◆ **Login Name** Specify the login name for the resource. For example, to access a resource on a network that requires authentication do one of the following:
  - ◆ **For Basic Authentication:** Specify the username.
  - ◆ **For Domain Authentication:** Specify the domain\username.
  - ◆ **For eDirectory Authentication:** Specify the Fully Qualified Distinguished Name in the following format:  
.username.ou.o  
For example: .jsmith.provo.novell  
However, the format `cn=jsmith,ou=provo,o=novell` is not supported.
- ◆ **Password** Specify the password for the resource's login name that you specified in the *Login Name* field.
- ◆ **Reenter Password** Re-enter the password for the resource's login name.




## 10.2 Creating a Folder for Credentials

- 1 In ZENworks Control Center, click the *Configuration* tab.



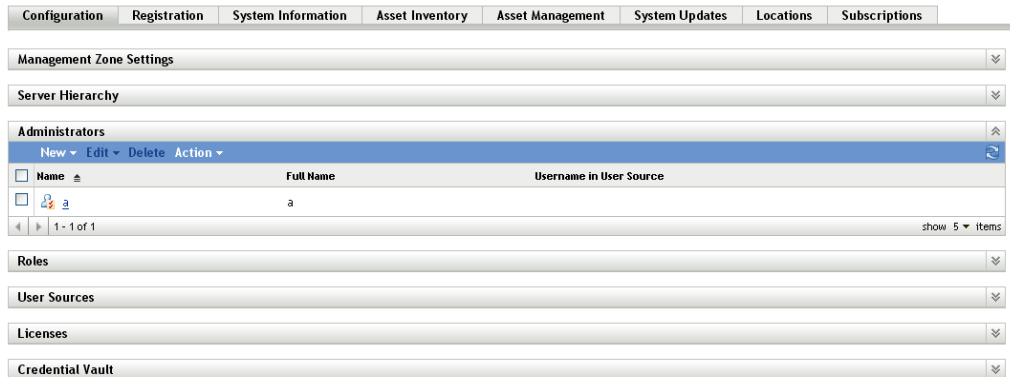
- 2 In the Credential Vault panel, click *New > Folder* to display the New Folder dialog box.

The screenshot shows the 'New Folder' dialog box. It has a title bar with a question mark and a close button. The dialog contains three fields: 'Name: \*' with an asterisk indicating it is required, 'Folder: \*' with an asterisk and a browse button (folder icon), and 'Description:'. Below the fields is a text area for the description. At the bottom, there is a note: 'Fields marked with an asterisk are required.' and two buttons: 'OK' and 'Cancel'.

- 3 In the *Name* field, specify a unique name for the folder.  
The folder cannot have the same name as any folders or credentials that already exist in the folder where you are creating it.
- 4 In the *Folder* field, click  to browse for and select the folder where you want the new folder created.
- 5 Type a description for the new folder, if desired.
- 6 Click *OK* to create the folder.

## 10.3 Assigning Credential Rights

- 1 In ZENworks Control Center, click the *Configuration* tab.



- 2 In the *Administrators* section, click the underlined link for the administrator for which you want to change rights.
- 3 Click the *Rights* tab.
- 4 In the *Assigned Rights* section, click *Add > Credential Rights*.
- 5 Click *Add* to select folders containing credentials, then modify the rights associated with those folders.

If you need help, click the *Help* button.

## 10.4 Editing a Credential


- 1 In ZENworks Control Center, click the *Configuration* tab.
- 2 In the Credential Vault panel, select the check box next to the credential.
- 3 Click *Edit*.
- 4 Edit the following fields.
  - ♦ **Credential Name:** Specify the name of the credential. When an action or task that requires authentication is executed, ZENworks uses this name to access the credential vault to obtain the resource's credentials.
  - ♦ **Description:** Provide an optional description of the credential.
  - ♦ **Login Name** Specify the login name for the resource. For example, to access a resource on a network that requires authentication do one of the following:
    - ♦ **For Basic Authentication:** Specify the username.
    - ♦ **For Domain Authentication:** Specify the domain\username.
    - ♦ **For eDirectory Authentication:** Specify the Fully Qualified Distinguished Name in the following format:  
.username.ou.o  
For example: .jsmith.provo.novell  
However, the format cn=jsmith,ou=provo,o=novell is not supported.
  - ♦ **Password** Specify the password for the resource's login name that you specified in the *Login Name* field.

- ♦ **Reenter Password** Re-enter the password for the resource's login name.
- 5 Click *OK*.

## 10.5 Renaming a Credential

- 1 In ZENworks Control Center, click the *Configuration* tab.
- 2 In the Credential Vault panel, select the check box next to the credential.
- 3 Click *Edit > Rename*.
- 4 Type the new name for the credential.
- 5 Click *OK*.

## 10.6 Moving a Credential to Another Folder

- 1 In ZENworks Control Center, click the *Configuration* tab.
- 2 In the Credential Vault panel, select the check box next to the credential.
- 3 Click *Edit > Move*.
- 4 In the *Folder* field, click  to browse for and select the folder where you want the credential moved.
- 5 Click *OK*.

## 10.7 Removing a Credential

- 1 In ZENworks Control Center, click the *Configuration* tab.
- 2 In the Credential Vault panel, select the check box next to the credential.
- 3 Click *Delete*.



---

# 11 Using Quick Tasks

Quick Tasks are the tasks that you can quickly perform on one or more devices through ZENworks Control Center.

Review the following sections:

- ♦ [Section 11.1, “Quick Tasks Types,” on page 93](#)
- ♦ [Section 11.2, “Initiating a Quick Task,” on page 95](#)
- ♦ [Section 11.3, “Cancelling, Stopping, or Hiding a Quick Task,” on page 97](#)

## 11.1 Quick Tasks Types

There are various quick tasks that you can perform on devices. Not all tasks are available for all objects (device, device group, device folder); unavailable tasks are dimmed in the ZENworks Control Center

After the quick task is invoked, you are prompted to specify the Primary Server to send the quick task notification and specify the quick task notification and expiry options. The status of the quick task is also displayed. For more information on the initiating the quick task options and viewing the quick task status, see [Section 11.2, “Initiating a Quick Task,” on page 95](#).

---

**NOTE:** The quick task options are not available for the Wake Up and Intel AMT Power Management quick task types.

---

The following list provides descriptions of the Quick Tasks you can perform:

- ♦ **Refresh Device:** Updates all information such as configuration settings, registration, and so forth) on the selected devices. In ZENworks Configuration, it updates the bundles and policies also.

---

**NOTE:** A Refresh Device quick task cannot be created for a device when another Refresh Device quick task is already active on the device. A Refresh Device quick task that is created for a group of devices is not assigned to the devices within the group that already have a Refresh Device quick task active on them.

---

- ♦ **Refresh Policies:** Updates policy information on the selected devices. This quick task is applicable for ZENworks Endpoint Security Management and ZENworks Configuration Management.
- ♦ **Clear ZESM User Defined Password:** Clears the user-defined secondary decryption password and the user-defined encryption/decryption password for removable storage devices. This quick task is applicable only for ZENworks Endpoint Security Management.
- ♦ **Clear ZESM Local Client Self Defense Settings:** Resets the Endpoint Security Agent to use the Client Self Defense settings contained within the device’s effective Security Settings policy. This overrides any local changes made to the settings. This quick task is applicable only for ZENworks Endpoint Security Management.

- ♦ **Clear ZESM Local Firewall Registration Settings:** Resets the Endpoint Security Agent to use the firewall registration settings contained within the device's effective Firewall policy. This overrides any local changes made to the settings. This quick task is applicable only for ZENworks Endpoint Security Management.
- ♦ **FDE - Decommission Full Disk Encryption:** Prevents access to a device's encrypted data by decommissioning the device disk. You can temporarily decommission the drive, in which case encrypted data is recoverable with a HelpDesk file or Emergency Recovery Disk, or you can permanently decommission the disk by erasing it. This quick task is applicable only for ZENworks Full Disk Encryption.
- ♦ **FDE - Enable Additive User Capturing:** Enables one-time user capturing. After the device receives this task, the user capture occurs at the next reboot. Whichever user logs in at that reboot is added to the PBA. To avoid possible security breaches and ensure the correct user capture, coordinate with the intended user when initiating this task. This quick task is applicable only for ZENworks Full Disk Encryption.
- ♦ **FDE - Force Device to Send ERI File to Server:** Instructs the device to send its Emergency Recovery Information (ERI) file to the ZENworks Server. This file is required to recover any temporarily decommissioned disk. This quick task is applicable only for ZENworks Full Disk Encryption.
- ♦ **FDE - Update PBA Password Settings:** Updates an existing user's PBA password or adds a new user (and password) to the PBA. This quick task is applicable only for ZENworks Full Disk Encryption.
- ♦ **Inventory Scan:** Initiates an inventory scan of the selected devices. For each device, the inventory scan uses the Scan Now settings defined for the device (*device view > Settings tab > Inventory*) to determine what information the scan collects.
- ♦ **Inventory Wizard:** Sends the inventory data collection form to the selected devices. For each device, the Inventory Collection Wizard uses the data collection form defined for the device (*device view > Settings tab > Inventory*).
- ♦ **Install Bundle:** Installs one or more bundles on the selected devices. This quick task is applicable only for ZENworks Configuration Management.
- ♦ **Uninstall Bundle:** Uninstalls one or more bundles on the selected devices. This quick task is applicable only for ZENworks Configuration Management.
- ♦ **Launch Bundle:** Launches one or more bundles on the selected devices. This quick task is applicable only for ZENworks Configuration Management.
- ♦ **Wake Up:** Uses Wake on LAN (WOL) technology to start a device that is shut down. The device must support WOL.
- ♦ **Intel AMT Power Management:** Allows you to change the power state of a device.
- ♦ **Reboot/Shutdown Devices:** Depending on your choice, shuts down or reboots the selected devices. You can include a warning message to be displayed on the devices. You can also specify a delay period for the reboot or shutdown.
- ♦ **Launch Application:** Launches an executable on the selected devices. The executable must be available to the devices either locally or in an accessible network location.
- ♦ **Run Script:** Runs a script on the selected devices. You can run a script that resides on the devices, resides on the your local drive, or that you intend to create. The script engine must be available to the devices either locally or in an accessible network location.
- ♦ **Launch Java Application:** Runs a Java application on the selected devices.
- ♦ **Retire Device Now:** Immediately retires the selected device from your ZENworks system. To retire a device at its next refresh, use the Retire Device action. Retiring a device is different from deleting a device. When you retire a device, its GUID is retained (as opposed to when you delete a device, which also deletes its GUID). As a result, all inventory information is retained and is

assessable. In ZENworks Configuration Management, all policy and bundle assignments are also removed. If you unretire the device in the future, its assignments are restored.

- ♦ **Unretire Device Now:** Immediately reactivates the selected device. In ZENworks Configuration Management, it reapplies all policy and bundle assignments that the device previously had. To unretire a device at its next refresh, use the Unretire Device action.

## 11.2 Initiating a Quick Task

Quick Tasks are available for the Devices, Bundles, and Policies lists in ZENworks Control Center. The following procedure provides an example of how to initiate a Quick Task from the Device list. The procedures for applying a Quick Task from the Bundles or Policies list is similar.

- 1 In ZENworks Control Center, click *Devices*, then locate the device to which you want to apply a Quick Task.
- 2 Select the check box next to the device, click *Quick Tasks*, then click *Refresh Policies* (or if you want to initiate a different Quick Task, click that task).
- 3 Configure the Quick Task options:

---

Option	Steps
Select the Primary Server to send the QuickTask notification	<p>Depending on the Primary Server that you want to send the quick task notification, do one of the following:</p> <ul style="list-style-type: none"><li>♦ <b>Current primary server:</b> Select this option to enable the Primary Server of the ZENworks Control Center that you are accessing to send the quick task notification.</li><li>♦ <b>Any primary server:</b> Select this option to enable any Primary Server in the Management Zone to send the quick task notification.  For example, you might want to use this option when the current Primary Server is busy performing other tasks.</li><li>♦ <b>Select one or more primary servers:</b> Select this option to choose one or more Primary Servers in the Management Zone to send the quick task notification.  For example, if you choose to use a single Primary Server to send the quick task notification to many devices, the workload on the server might increase because it must send the notification to all the devices. You can select multiple Primary Servers so that the load of notifying many devices is distributed among the servers.  Click <i>Add</i> to select and add the Primary Servers. Click <i>Remove</i> to remove any previously added Primary Server.</li></ul>

---

Option	Steps
QuickTask Notification Options	<p>Select one of the following:</p> <ul style="list-style-type: none"> <li>◆ <b>Notify all the devices immediately:</b> Select this option to send the quick task notification to all the devices immediately. For example, you might want to select this option when the quick task notification is sent to a smaller number of devices and the Primary Server can handle all the quick task requests from all the devices at the same time.</li> <li>◆ <b>Notify all the devices within _ mins:</b> Select this option to send the quick task notification to all the devices within the specified time. By default, the notification time is set to 5 minutes. You can choose to specify the notification time according to your requirements. For example, you might want to select this option when the quick task notification is sent to a larger number of devices and the Primary Server might not be able to handle all the quick task requests from all the devices at the same time.</li> </ul>
QuickTask Expiry Option	<p>Select one of the following:</p> <ul style="list-style-type: none"> <li>◆ <b>Expires immediately when failed to notify the device:</b> Select this option to immediately expire the quick task when the quick task notification to the devices fails. For example, you might want to select this option to send a <i>Reboot/Shut Down Devices</i> quick task for rebooting or shutting down a device. If the device is already shut down, you don't want to execute the quick task on the device when the device restarts.</li> <li>◆ <b>Never Expires:</b> Select this option if you never want the quick task to expire. For example, you might want to select this option when you send an <i>Install Bundle</i> quick task to install an application on a device that might not be running at that time.</li> <li>◆ <b>Expires after _ mins of the quick task creation:</b> Select this option to expire the quick task a certain amount of time after it is created. By default, the expiry time is set to 5 minutes. You can choose to specify the expiration time according to your requirement. For example, you might want to select this option when you need to launch an application on multiple devices that are either in the process of booting up or are likely to be started within the stipulated time.</li> </ul>

- 4 Click *Start* to initiate the notification of the quick task.
- 5 Click the QuickTask Status tab to monitor the status of the task.

Status	Description
New	The Primary Server has not started the process of notifying the device.
Connecting	The Primary Server is attempting to connect to the device.
Connected	The Primary Server is connected to the device.
Connection Failed	The Primary Server is unable to connect to the device.



---

Status	Description
Connection Failed (Expired)	The Primary Server is unable to connect to the device and the quick task assignment has expired.
Stopped	The quick task notification was stopped before it was sent to the device. You can do this only if the quick task has not yet been assigned to the device.
Assigned	The quick task has been assigned to the device.
Done	The quick task has been executed on the device.

---

## 11.3 Cancelling, Stopping, or Hiding a Quick Task

- ♦ To stop the quick task on a managed device, select the device on which you want to stop the quick task and click *Stop*. You can do this only if the quick task has not yet been assigned to the device.
- ♦ To hide the quick task dialog box, click *Hide*. The quick task is listed in the Quick Tasks list in the left navigation pane, and you can click the quick task to check the status again.
- ♦ To cancel the quick task, click *Cancel*.



---

# 12 Using System Variables

System variables let you define variables that can be used to replace paths, names, and so forth as you enter information in ZENworks Control Center.

You can define system variables at three levels:

- ♦ **Management Zone:** The system variables are inherited by all device folders, devices, and bundles.
- ♦ **Device Folder:** The system variables are inherited by all devices contained within the folder or its subfolders.
- ♦ **Device or Bundle:** The system variables apply only to the device or bundle for which they are configured.

The following sections contain more information:

- ♦ [Section 12.1, “Understanding System Variables,” on page 99](#)
- ♦ [Section 12.2, “Adding System Variables,” on page 100](#)
- ♦ [Section 12.3, “Removing System Variables,” on page 101](#)
- ♦ [Section 12.4, “Editing System Variables,” on page 101](#)
- ♦ [Section 12.5, “Using System Variables,” on page 101](#)

## 12.1 Understanding System Variables

The following examples illustrate some uses of system variables:

- ♦ **Specifying Paths and Filenames in Actions:** When you create an Edit INI File action, for example, you specify a `.ini` file and configure the changes to be performed on that file. During the creation process, you can specify the full path to the file (for example, `C:\Program Files\OpenOffice.org 2.0\program\setup.ini`).

Instead of specifying the entire path and filename, you can create a system variable. For example, the name of the variable can be `OpenOffice INI` and the value can be the full path to the file. Now, instead of specifying the full path and filename when you create the action, you can type `${OpenOffice INI}` in the *Filename* field.

An advantage of using a system variable rather than typing the full path and filename is that you can specify this particular `.ini` file in many different types of actions. Suppose that the location of the `.ini` file changes. Instead of editing the path in each action, you can edit the path in the system variable and all the actions still point to the correct path.

You can generalize the path even more by creating a system variable named `ProgramFiles` with the value of `C:\program files`. In the future, when you specify a path, you can type `${ProgramFiles}` and then specify the remaining path to the specific file. For example,

`${ProgramFiles}\OpenOffice 2.0\program\setup.ini`. Again, if the path to the `C:\program` files directory changes in the future, you only need to change the path in the system variable, rather than in each bundle that uses that location in a path.

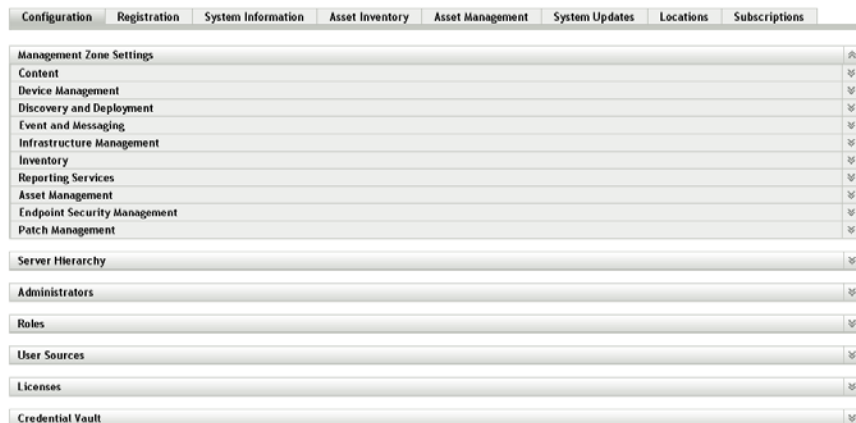
- ♦ **Overriding Inherited Settings:** When configuring system variables for a folder, device, or bundle, you can override an inherited variable by defining a new variable with the same name but a different value. For example, if `ProgramFiles=C:\` is defined at the Management Zone, you can override it by defining `ProgramFiles=D:\` at the device folder level or at the device or bundle.

You can use a system variable when creating a bundle. Depending on the location of the targeted device object in the folder hierarchy, the value can be different.

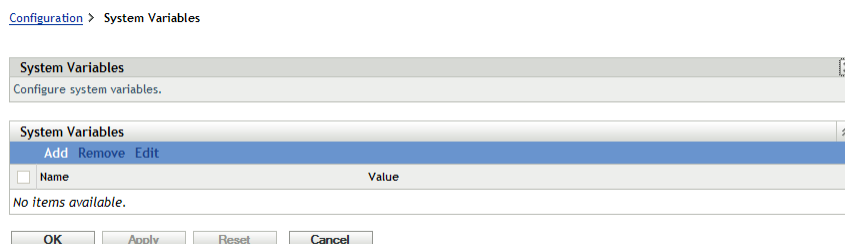
For example, suppose that all of your applications are installed in `C:\program` files except for specific applications used by the accounting department, which are installed in `D:\program` files. You define the `ProgramFiles` variable at the Management Zone level to point to `C:\program` files. For the accounting applications, you create a device folder called `Accounting Department` to contain the devices in the accounting department. You can set the value for the `ProgramFiles` variable to `D:\program` files on the `Accounting Department` device folder level. When the same bundle is applied to devices, the path to the program files directory is on the `C:\` drive for all targeted devices except for those contained in the `Accounting Department` device folder. For those devices, the program files directory points to the `D:\` drive.

## 12.2 Adding System Variables

- 1 In ZENworks Control Center, click the *Configuration* tab.



- 2 In the Management Zone Settings list, click *Device Management*.
- 3 Click *System Variables*.



- 4 Click *Add*, provide the name and value for the variable, then click *OK*.

When configuring system variables for a folder, device, or bundle, you can override an inherited variable by defining a new variable with the same name but a different value. For example, if `Var1=c:\` is inherited, you can override it by defining `Var1=d:\`.

Variable names cannot include spaces and must be unique at the level where they are defined. For example, you cannot have two variables named `Var1` defined at the device level (unless one is inherited, in which case the device-level variable overrides the inherited variable).

Variable values cannot include the characters `&` and `<`.

- 5 Click *Apply*.

## 12.3 Removing System Variables

- 1 In ZENworks Control Center, click the *Configuration* tab.
- 2 In the *Management Zone Settings* list, click *Device Management*.
- 3 Click *System Variables*.
- 4 Select the check box next to the variable (or variables).
- 5 Click *Remove*.
- 6 Click *Apply*.

## 12.4 Editing System Variables

- 1 In ZENworks Control Center, click the *Configuration* tab.
- 2 In the *Management Zone Settings* list, click *Device Management*.
- 3 Click *System Variables*.
- 4 Select the check box next to the variable, then click *Edit*.
- 5 Modify the *Name* and *Value* fields as desired, then click *OK*.
- 6 Click *Apply*.

## 12.5 Using System Variables

- 1 Use the following syntax:

```
${VAR_NAME}
```

Replace `VAR_NAME` with the name of the variable.



---

# 13 Using Special System Variables

The following sections contain information on the special system variables supported in Novell ZENworks Configuration Management:

- ◆ [Section 13.1, “Windows Special System Variables,” on page 103](#)
- ◆ [Section 13.2, “Login Script Special System Variables,” on page 108](#)
- ◆ [Section 13.3, “Novell eDirectory Attribute Special System Variables,” on page 109](#)
- ◆ [Section 13.4, “Microsoft Active Directory Attribute Special System Variables,” on page 112](#)
- ◆ [Section 13.5, “Language Variable Special System Variables,” on page 114](#)

## 13.1 Windows Special System Variables

A Windows special system variable is one that defines the Windows directories. The typical paths listed below are based on default installations and might not match your specific setup.

Suppose that you have installed Windows to drive D: (for example, D:\WINDOWS). However, an application installation expects Windows to be on drive C: (for example, C:\WINDOWS). You can use the WinDisk system variable to substitute drive D: for the files that require it.

**Table 13-1** Windows System Variables

Macro	Description
<code>\${AdminTools}</code>	<p>File system directory that contains the administrative tools that appear in the Control Panel when a specific user logs on to the device.</p> <p>On a Windows Server 2003 or Windows XP device, it is typically C:\Documents and Settings\Username\Start Menu\Programs\Administrative Tools.</p> <p>On a Windows Server 2008, Windows Vista, or Windows 7 device, it is typically C:\Users\Username\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Administrative Tools.</p>
<code>\${AllUsersProfile}</code>	<p>File system directory that contains common profile for all the users.</p> <p>On a Windows Server 2003 or Windows XP device, it is typically C:\Documents and Settings\All Users.</p> <p>On a Windows Server 2008, Windows Vista, or Windows 7 device, it is typically C:\ProgramData.</p>

<b>Macro</b>	<b>Description</b>
<code>\${AppData}</code>	<p>File system directory that serves as a common repository for application-specific data.</p> <p>On a Windows Server 2003 or Windows XP device, it is typically <code>C:\Documents and Settings\Username\Application Data</code>.</p> <p>On a Windows Server 2008, Windows Vista, or Windows 7 device, it is typically <code>C:\Users\Username\AppData\Roaming</code>.</p>
<code>\${CommonDesktop}</code>	<p>File system directory that contains files and folders that appear on the desktop for all users.</p> <p>On a Windows Server 2003 or Windows XP device, it is typically <code>C:\Documents and Settings\All Users\Desktop</code>.</p> <p>On a Windows Server 2008, Windows Vista, or Windows 7 device, it is typically <code>C:\Users\Public\Desktop</code>.</p>
<code>\${CommonPrograms}</code>	<p>File system directory that contains the directories for the common program groups that appear on the Start menu for all users.</p> <p>On a Windows Server 2003 or Windows XP device, it is typically <code>C:\Documents and Settings\All Users\Start Menu\Programs</code>.</p> <p>On a Windows Server 2008, Windows Vista, or Windows 7 device, it is typically <code>C:\ProgramData\Microsoft\Windows\Start Menu\Programs</code>.</p>
<code>\${CommonStartMenu}</code>	<p>File system directory that contains the programs and folders that appear on the Start menu for all users.</p> <p>On a Windows Server 2003 or Windows XP device, it is typically <code>C:\Documents and Settings\All Users\Start Menu</code>.</p> <p>On a Windows Server 2008, Windows Vista, or Windows 7 device, it is typically <code>C:\ProgramData\Microsoft\Windows\Start Menu</code>.</p>
<code>\${CommonStartup}</code>	<p>File system directory that contains the programs that appear in the Startup folder for all users. The system starts these programs whenever any user logs on.</p> <p>On a Windows Server 2003 or Windows XP device, typically this directory is <code>C:\Documents and Settings\All Users\Start Menu\Programs\Startup</code>.</p> <p>On a Windows Server 2008, Windows Vista, or Windows 7 device, typically this directory is <code>C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup</code>.</p>
<code>\${CommonAdminTools}</code>	<p>File system directory that contains the administrative tools that appear in the Control Panel for all users who logs in to the device.</p> <p>On a Windows Server 2003 or Windows XP device, it is typically <code>C:\Documents and Settings\All Users\Start Menu\Programs\Administrative Tools</code>.</p> <p>On a Windows Server 2008, Windows Vista, or Windows 7 device, it is typically <code>C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Administrative Tools</code>.</p>



<b>Macro</b>	<b>Description</b>
<code>#{CommonAppData}</code>	<p>File system directory that contains the application-specific data for all users who logs in to the device.</p> <p>On a Windows Server 2003 or Windows XP device, it is typically <code>C:\Documents and Settings\All Users\Application Data</code>.</p> <p>On a Windows Server 2008, Windows Vista, or Windows 7 device, it is typically <code>C:\ProgramData</code>.</p>
<code>#{CommonDocuments}</code>	<p>File system directory that contains the documents shared by all users who log in to the device.</p> <p>On a Windows Server 2003 or Windows XP device, it is typically <code>C:\Documents and Settings\All Users\Documents</code>.</p> <p>On a Windows Server 2008, Windows Vista, or Windows 7 device, it is typically <code>C:\Users\Public\Documents</code>.</p>
<code>#{CommonProgramFiles}</code>	<p>File system directory that contains the program files shared by multiple applications.</p> <p>On a Windows Server 2008, Windows Vista, or Windows 7 device, it is typically <code>C:\Program Files\Common Files</code>.</p>
<code>#{CommonTemplates}</code>	<p>File system directory that contains the document templates shared by all users who log in to the device.</p> <p>On a Windows Server 2003 or Windows XP device, it is typically <code>C:\Documents and Settings\All Users\Templates</code>.</p> <p>On a Windows Server 2008, Windows Vista, or Windows 7 device, it is typically <code>C:\ProgramData\Microsoft\Windows\Templates</code>.</p>
<code>#{Cookies}</code>	<p>Files system directory that contains the user's cookies.</p> <p>On a Windows Server 2003 or Windows XP device, it is typically <code>C:\Documents and Settings\Username\Cookies</code>.</p> <p>On a Windows Server 2008, Windows Vista, or Windows 7 device, it is typically <code>C:\Users\Username\AppData\Roaming\Microsoft\Windows\Cookies</code>.</p>
<code>#{Desktop}</code>	<p>File system directory used to physically store file objects on the desktop (not the desktop folder itself).</p> <p>On a Windows Server 2003 or Windows XP device, typically this directory is <code>C:\Documents and Settings\Username\Desktop</code>.</p> <p>On a Windows Server 2008, Windows Vista, or Windows 7 device, typically this directory is <code>C:\Users\Username\Desktop</code>.</p>
<code>#{Favorites}</code>	<p>File system directory that serves as a common repository for the user's favorite items.</p> <p>On a Windows Server 2003 or Windows XP device, typically this directory is <code>C:\Documents and Settings\Username\Favorites</code>.</p> <p>On a Windows Server 2008, Windows Vista, or Windows 7 device, typically this directory is <code>C:\Users\Username\Favorites</code>.</p>
<code>#{Fonts}</code>	<p>Virtual folder containing fonts. Typically <code>C:\Windows\Fonts</code>.</p>

<b>Macro</b>	<b>Description</b>
<code>\$(History)</code>	<p>File system directory that contains the user's history of visited Internet addresses.</p> <p>On a Windows Server 2003 or Windows XP device, it is typically <code>C:\Documents and Settings\Username\Local Settings\History</code>.</p> <p>On a Windows Server 2008, Windows Vista, or Windows 7 device, it is typically <code>C:\Users\Username\AppData\Local\Microsoft\Windows\History</code>.</p>
<code>\$(LocalAppData)</code>	<p>File system directory that serves as a common repository for application-specific data.</p> <p>On a Windows Server 2008, Windows Vista, or Windows 7 device, it is typically, <code>C:\Users\Username\AppData\Local</code>.</p>
<code>\$(MyPictures)</code>	<p>File system directory that contains a specific user's graphics files.</p> <p>On a Windows Server 2003 or Windows XP device, it is typically <code>c:\Documents and Settings\Username\My Documents\My Pictures</code>.</p> <p>On a Windows Server 2008, Windows Vista, or Windows 7 device, it is typically <code>c:\Users\Username\Pictures</code>.</p>
<code>\$(NetHood)</code>	<p>File system directory containing objects that appear in the network neighborhood.</p> <p>On a Windows Server 2003 or Windows XP device, it is typically <code>C:\Documents and Settings\Username\NetHood</code>.</p> <p>On a Windows Server 2008, Windows Vista, or Windows 7 device, it is typically <code>C:\Users\Username\Roaming\Microsoft\Windows\Network Shortcuts</code>.</p>
<code>\$(Personal)</code>	<p>File system directory that serves as a common repository for documents.</p> <p>On a Windows Server 2003 or Windows XP device, it is typically <code>C:\Documents and Settings\Username\My Documents</code>.</p> <p>On a Windows Server 2008, Windows Vista, or Windows 7 device, it is typically <code>C:\Users\Username\Documents</code>.</p>
<code>\$(PrintHood)</code>	<p>File system directory that serves as a common repository for printer links.</p> <p>On a Windows Server 2003 or Windows XP device, it is typically <code>C:\Documents and Settings\Username\PrintHood</code>.</p> <p>On a Windows Server 2008, Windows Vista, or Windows 7 device, it is typically <code>C:\Users\Username\AppData\Roaming\Microsoft\Windows\Printer Shortcuts</code>.</p>
<code>\$(Programs)</code>	<p>File system directory that contains the user's program groups, which are also file system directories.</p> <p>On a Windows Server 2003 or Windows XP device, it is typically <code>C:\Documents and Settings\Username\Start Menu\Programs</code>.</p> <p>On a Windows Server 2008, Windows Vista, or Windows 7 device, it is typically <code>C:\Users\Username\AppData\Roaming\Microsoft\Windows\Start Menu\Programs</code>.</p>

Macro	Description
<code>\${ProgramData}</code>	<p>File system directory that contains the user's program groups, which are also file system directories.</p> <p>On a Windows Server 2008, Windows Vista, or Windows 7 device, it is typically <code>C:\ProgramData</code>.</p>
<code>\${ProgramFiles}</code>	<p>File system directory that contains the user's program files on a 32-bit device or the user's 64-bit program files on a 64-bit device.</p> <p>Typically <code>C:\Program Files</code>.</p>
<code>\${ProgramFiles32}</code>	<p>File system directory that contains the user's 32-bit program files on a 64-bit device. Typically <code>C:\Program Files(x86)</code>.</p>
<code>\${ProgramFilesCommon}</code>	<p>File system directory that contains the program files shared by multiple applications. Typically <code>C:\Program Files\Common Files</code>.</p>
<code>\${Public}</code>	<p>File system directory that has public access to all the users on the network.</p> <p>On a Windows Server 2008, Windows Vista, or Windows 7 device, it is typically <code>C:\Users\Public</code>.</p>
<code>\${Recent}</code>	<p>File system directory that contains the user's most recently used documents.</p> <p>On a Windows Server 2003 or Windows XP device, it is typically <code>C:\Documents and Settings\Username\Recent</code>.</p> <p>On a Windows Server 2008, Windows Vista, or Windows 7 device, it is typically <code>C:\Users\Username\AppData\Roaming\Microsoft\Windows\Recent</code></p>
<code>\${SendTo}</code>	<p>File system directory that contains Send To menu items.</p> <p>On a Windows Server 2003 or Windows XP device, it is typically <code>C:\Documents and Settings\Username\SendTo</code>.</p> <p>On a Windows Server 2008, Windows Vista, or Windows 7 device, it is typically <code>C:\Users\username\AppData\Roaming\Microsoft\Windows\SendTo</code></p>
<code>\${StartMenu}</code>	<p>File system directory containing <i>Start</i> menu items.</p> <p>On a Windows Server 2003 or Windows XP device, it is typically <code>C:\Documents and Settings\Username\Start Menu</code>.</p> <p>On a Windows Server 2008, Windows Vista, or Windows 7 device, it is typically <code>C:\Users\Username\AppData\Roaming\Microsoft\Windows\Start Menu</code>.</p>
<code>\${Startup}</code>	<p>File system directory that corresponds to the user's Startup program group.</p> <p>On a Windows Server 2003 or Windows XP device, it is typically <code>C:\Documents and Settings\Username\Start Menu\Programs\Startup</code>.</p> <p>On a Windows Server 2008, Windows Vista, or Windows 7 device, it is typically <code>C:\Users\Username\AppData\Roaming\Microsoft\Windows\Startup</code>.</p>

Macro	Description
<code>\${TempDir}</code>	Windows temporary directory.  On a Windows Server 2003 or Windows XP device, it is typically <code>C:\Documents and Settings\Username\Local Settings\Temp</code> .  On a Windows Server 2008, Windows Vista, or Windows 7 device, it is typically <code>C:\Users\Username\AppData\Local\Temp</code> .
<code>\${Templates}</code>	File system directory that serves as a common repository for document templates.  On a Windows Server 2003 or Windows XP device, it is typically <code>C:\Documents and Settings\Username\Templates</code> .  On a Windows Server 2008, Windows Vista, or Windows 7 device, it is typically <code>C:\Users\Username\AppData\Roaming\Microsoft\Windows\Templates</code> .
<code>\${UserProfile}</code>	File system directory that contains the logged-in user's profile.  On a Windows Server 2003 or Windows XP device, it is typically <code>C:\Documents and Settings\Username</code> .  On a Windows Server 2008, Windows Vista, or Windows 7 device, it is typically <code>C:\Users\Username</code> .
<code>\${WinDesktop}</code>	Windows desktop directory  On a Windows Server 2003 or Windows XP device, it is typically <code>C:\Documents and Settings\Username\Desktop</code> .  On a Windows Server 2008, Windows Vista, or Windows 7 device, it is typically <code>C:\Users\Username\Desktop</code> .
<code>\${WinDir}</code>	Windows directory. Typically <code>C:\WINDOWS</code> .
<code>\${WinDisk}</code>	Drive letter (plus colon) for the Windows directory. Typically <code>C:</code> .
<code>\${WinSysDir}</code>	Windows system directory. Typically <code>C:\WINDOWS\system32</code> .
<code>\${WinSysDisk}</code>	Drive letter (plus colon) for the Windows system directory. Typically <code>C:</code> .

**NOTE:** For compatibility with traditional ZENworks, the system variable can also be specified in one of the following formats:

- ◆ `%system_variable%`  
For example, `%ProgramFiles%`
- ◆ `.*system_variable%`  
For example, `.*ProgramFiles%`

## 13.2 Login Script Special System Variables

The following table lists the supported login script special system variables:

**Table 13-2** Supported Login Script Special System Variables

Macro	Description
<code>\${COMPUTER_NAME}</code>	The name of the computer. For example: work_pc.
<code>\${DAY}</code>	Numeric day of the month. For example: 01, 10, 15.
<code>\${HOUR24}</code>	Time of the day according to a 24-hour clock. For example: 02, 05, 14, 22.
<code>\${HOUR}</code>	Hour of the day. For example: 0 = 12, 13 = 1.
<code>\${LAST_NAME}</code>	Last name of the current user (also known as the user's eDirectory Surname attribute). For example: Jones.
<code>\${MINUTE}</code>	Current minute. For example: 02, 59.
<code>\${MONTH}</code>	Current month number. For example: 01 for January.
<code>\${NDAY_OF_WEEK}</code>	Numeric day of the week. For example: 1 for Sunday, 2 for Monday.
<code>\${NETWORK}</code>	Workstation network address. For example: 101.10.101.101
<code>\${OS_VERSION}</code>	Version of the OS. For example: v5.00.
<code>\${OS}</code>	OS type. For example: MSDOS, WIN98, WINNT, WIN2000, WINXP.
<code>\${PLATFORM}</code>	Platform running. For example: WIN32NT.
<code>\${PHYSICAL_STATION}</code>	MAC address. For example: 0000C04FD92ECA.
<code>\${SECOND}</code>	Number of seconds. For example: 03, 54.
<code>\${SHORT_YEAR}</code>	Short year number. For example: 97, 00.
<code>\${WINVER}</code>	Windows version. For example: v3.11, v4.00.
<code>\${YEAR}</code>	Full year number. For example: 2008.

**NOTE:** For compatibility with traditional ZENworks, the system variable can also be specified in one of the following formats:

- ♦ `%system_variable%`  
For example, %MONTH%
- ♦ `;%*system_variable%`  
For example, %\*MONTH%

## 13.3 Novell eDirectory Attribute Special System Variables

The ZENworks Application Window supports system variables that pull information from the attributes of the currently logged-in user.

The following sections explain the system variable syntax and provide examples:

- ♦ [Section 13.3.1, "Syntax," on page 110](#)
- ♦ [Section 13.3.2, "Examples," on page 110](#)
- ♦ [Section 13.3.3, "Configuring the eDirectory Attribute Special System Variables," on page 111](#)

## 13.3.1 Syntax

eDirectory attribute system variables use the following syntax:

```
%eDirectory_attribute%
```

**Table 13-3** Special System Variable Syntax

Element	Description
%	Flags the text as a system variable. The entire system variable must be enclosed in% characters.
eDirectory_attribute	Defines the attribute to be read.  You can use the ConsoleOne Schema Manager (available from the Tools menu) to view an eDirectory object's available attributes.

## 13.3.2 Examples

The following table provides examples of eDirectory attribute system variables.

**Table 13-4** Special System Variable Examples

Macro	Description
%CN%	Returns the common name of the currently logged-in user.
%DN%	Returns the distinguished name of the currently logged-in user.
%Full Name%	Returns the full name of the currently logged-in user. This is the name defined in User object > General tab > Identification page > Full Name field.
%Given Name%	Returns the first name of the currently logged-in user. This is the name defined in User object > General tab > Identification page > Given Name field.
%Surname%	Returns the last name of the currently logged-in user. This is the name defined in the User object > General tab > Identification page > Last Name field.

The remaining system variables that are predefined by ZENworks are available in the following locations:

- ♦ **On Windows:** `ZENworks_Home/novell/zenworks/datamodel/authsource/edirectory-users.zls.xml`
- ♦ **On Linux:** `/etc/opt/novell/zenworks/datamodel/authsource/edirectory-users.zls.xml`

**NOTE:** For compatibility with traditional ZENworks, the special system variables can also be specified in one of the following formats:

- ♦ `%system_variable%`

For example, `%CN%`

- ♦ `%*system_variable%`  
For example, `%*CN%`
- 

### 13.3.3 Configuring the eDirectory Attribute Special System Variables

To use eDirectory attributes as a reference in the bundle system variables, use the following procedures:

#### On the eDirectory Server

Define a name mapping between LDAP attribute types and eDirectory attribute definitions. You can log in to Novell iManager and click *Attribute Map* to do the mapping. For example, you can choose to map an eDirectory attribute named `GWMailID`, which stores the user e-mail id, to a Primary LDAP Attribute named `Mail`.

Only User attributes are supported.

For information on mapping the LDAP attribute types and eDirectory attribute, see Novell eDirectory Administration guide at the [Novell Documentation Website \(http://www.novell.com/documentation/\)](http://www.novell.com/documentation/).

#### On the ZENworks Server

- 1 Edit the sample file to create a file that contains the attribute that you want to use with ZENworks:
  - ♦ **On Windows:** `ZENworks_Home/novell/zenworks/datamodel/authsource/edirectory-users-additional.zls.xml.sample`
  - ♦ **On Linux:** `/etc/opt/novell/zenworks/datamodel/authsource/edirectory-users-additional.zls.xml.sample`
- 2 Add an entry for the attribute that you want to use with ZENworks. For example:

```
<attribute name="ZEN" ldapName="Mail"
builder="com.novell.zenworks.datamodel.session.jndi.builder.StringAttributeBuilder" />
```

Replace `ZEN` with the attribute that you want to use with ZENworks and replace `Mail` with the Primary LDAP Attribute that you mapped with the eDirectory attribute named `GWMailID`.

You must use the right builder, depending on whether the syntax is a string, integer, or Boolean. The `edirectory-users-additional.zls.xml.sample` file lists the different type of builders.
- 3 Save the sample file as `edirectory-users-additional.zls.xml`.
- 4 Replace the `edirectory-users-additional.zls.xml` file on all the Primary Servers in the Management Zone.
- 5 Restart the `zenserver` service.

#### Sample Scenario

Create a bundle with an action that references the macro and that runs in the user impersonation mode. For example:

1. Create a bundle with a Run Script action that references the special system variable, `${ZEN}` and has the executable security level set to `Run as logged in user`.

2. Perform the bundle assignment.

When the action is executed on the managed device, the value of the LDAP attribute is substituted for the special system variable.

In the example, the email id stored in the `GWMailID` attribute is substituted for the special system variable, `${ZEN}`. Consequently, when the action is executed on the managed device, the e-mail ID stored in the `GWMailID` attribute is displayed on the device.

## 13.4 Microsoft Active Directory Attribute Special System Variables

The ZENworks Application Window supports special system variables that pull information from the attributes of the currently logged-in user.

The following sections explain the system variable syntax and provide examples:

- ♦ [Section 13.4.1, “Syntax,” on page 112](#)
- ♦ [Section 13.4.2, “Examples,” on page 112](#)
- ♦ [Section 13.4.3, “Configuring the Active Directory Attribute Special System Variables,” on page 113](#)

### 13.4.1 Syntax

Active Directory attribute special system variables use the following syntax:

```
%active-directory_attribute%
```

**Table 13-5** *Special System Variable Syntax*

Element	Description
%	Flags the text as a system variable. The entire system variable must be enclosed in% characters.
active-directory_attribute	Defines the attribute to be read.

### 13.4.2 Examples

The following table provides examples of Active Directory attribute system variables.

**Table 13-6** *Special System Variable Examples*

Special System Variables	Description
%CN%	Returns the common name of the currently logged-in user.
%OU%	Returns the organizational unit name for the currently logged-in user.
%Full Name%	Returns the full name of the currently logged-in user.
%Surname%	Returns the last name of the currently logged-in user.



Special System Variables	Description
%Street%	Returns the street address of the currently logged-in user.

The remaining special system variables that are predefined by ZENworks are available in the following locations:

- ♦ **On Windows:** *ZENworks\_Home*/novell/zenworks/datamodel/authsource/active-directory-users.zls.xml
- ♦ **On Linux:** /etc/opt/novell/zenworks/datamodel/authsource/active-directory-users.zls.xml

### 13.4.3 Configuring the Active Directory Attribute Special System Variables

To use Active Directory attributes as a reference in the special system variables, use the following procedures:

#### On the Active Directory Server

To map existing or new attributes defined in the Active Directory schema, see the [Microsoft TechNet Library](http://technet.microsoft.com/en-us/library/cc961581.aspx) (<http://technet.microsoft.com/en-us/library/cc961581.aspx>).

#### On the ZENworks Server

- 1 Edit the sample file to create a file that contains the attribute that you want to use with ZENworks:
  - ♦ **On Windows:** *ZENworks\_Home*/novell/zenworks/datamodel/authsource/active-directory-users-additional.zls.xml.sample
  - ♦ **On Linux:** /etc/opt/novell/zenworks/datamodel/authsource/active-directory-users-additional.zls.xml.sample

- 2 Add an entry for the attribute that you want to use with ZENworks. For example:

```
<attribute name="ZEN" ldapName="employeeID"
builder="com.novell.zenworks.datamodel.session.jndi.builder.StringAttributeBuilder" />
```

Replace `ZEN` with the attribute that you want to use with ZENworks and replace `EmployeeID` with the LDAP Display Name in Active Directory. If the Active Directory common name for this attribute is defined as `Employee-ID`, `ZEN` now maps to the attribute `Employee-ID`.

You must use the right builder, depending on whether the syntax is a string, integer, or Boolean. The `active-directory-users-additional.zls.xml.sample` file lists the different type of builders.

- 3 Save the sample file as `active-directory-users-additional.zls.xml`.
- 4 Replace the `active-directory-users-additional.zls.xml` file on all the Primary Servers in the Management Zone.
- 5 Restart the `zenserver` service.

## Sample Scenario

Create a bundle with an action that references the special system variable and that runs in the user impersonation mode. For example:

1. Create a bundle with a Run Script action that references the special system variable `${ZEN}` and has the executable security level set to `Run as logged in user`.
2. Perform the bundle assignment.

When the action is executed on the managed device, the value of the LDAP attribute is substituted for the special system variable.

In the example, the employee id stored in the `Employee-ID` attribute is substituted for the special system variable, `${ZEN}`. Consequently, when the action is executed on the managed device, the employee ID stored in the `Employee-ID` attribute is displayed on the device.

## 13.5 Language Variable Special System Variables

To minimize the number of Application objects required to distribute the same application in different languages, you can use language variables to represent language-related information in MSI Application objects.

The following table describes the available language variables:

**Table 13-7** Language Variable Special System Variables

Language Variable	Description
<code>%LOCALE_SYS_DEFAULT_ANSI_CP%</code>	Retrieves the American National Standards Institute (ANSI) code page associated with the system locale. If the locale does not use an ANSI code page, the value is 0.  Example: 1252
<code>%LOCALE_SYS_DEFAULT_OEM_CP%</code>	Retrieves the original equipment manufacturer (OEM) code page associated with the system locale. If the locale does not use an OEM code page, the value is 1.  Example: 437
<code>%LOCALE_SYS_LANGID%</code>	Retrieves the language identifier for the system locale. The language identifier is a standard international numeric abbreviation for the language in a country or geographical region.  Example: 0409
<code>%LOCALE_SYS_ABBR_LANG%</code>	Specifies the abbreviated name of the system language. In most cases, it is created by taking the two-letter language abbreviation from the International Organization for Standardization (ISO) Standard 639 and adding a third letter, as appropriate, to indicate the sub language.  Example: ENU

Language Variable	Description
%LOCALE_SYS_ENG_LANG%	<p>Specifies the full English name of the system language from ISO Standard 639. This is always restricted to characters that can be mapped into the ASCII 127-character subset.</p> <p>Example: English</p>
%LOCALE_SYS_LANG%	<p>Specifies the full localized name of the system language. This name is based on the localization of the product and might vary for each localized version.</p> <p>Example: English (United States)</p>
%LOCALE_SYS_ISO639_LANG%	<p>Specifies the abbreviated name of the system language based only on ISO Standard 639.</p> <p>Example: en</p>
%LOCALE_SYS_NATIVE_LANG%	<p>Specifies the native name of the system language.</p> <p>Example: English</p>
%LOCALE_USER_DEFAULT_ANSI_CP%	<p>Retrieves the American National Standards Institute (ANSI) code page associated with the user locale. If the locale does not use an ANSI code page, the value is 0.</p> <p>Example: 1252</p>
%LOCALE_USER_DEFAULT_OEM_CP%	<p>Retrieves the original equipment manufacturer (OEM) code page associated with the user locale. If the locale does not use an OEM code page, the value is 1.</p> <p>Example: 850</p>
%LOCALE_USER_LANGID%	<p>Retrieves the language identifier for the user locale. The language identifier is a standard international numeric abbreviation for the language in a country or geographical region.</p> <p>Example: 0c09</p>
%LOCALE_USER_ENG_LANG%	<p>Specifies the full English name of the user language from ISO Standard 639. This is always restricted to characters that can be mapped into the ASCII 127-character subset.</p> <p>Example: English</p>
%LOCALE_USER_LANG%	<p>Specifies the full localized name of the user language. This name is based on the localization of the product and might vary for each localized version.</p> <p>Example: English (Australia)</p>
%LOCALE_USER_ISO639_LANG%	<p>Specifies the abbreviated name of the user language based only on ISO Standard 639.</p> <p>Example: en</p>
%LOCALE_USER_NATIVE_LANG%	<p>Specifies the native name of the user language.</p> <p>Example: English</p>



---

# 14 Troubleshooting ZENworks Control Center

- ♦ “An HTTP request is not redirected to HTTPS if IIS is running on the Primary Server” on page 117
- ♦ “ZENworks Control Center throws a `java.lang.NoClassDefFoundError` Exception” on page 117
- ♦ “Opening links in a new tab or new window of ZENworks Control Center might fail to display the page” on page 118
- ♦ “Logging in to ZENworks Control Center or navigating within ZENworks Control Center by using Firefox 3.x might display a blank page” on page 118
- ♦ “ZENworks Control Center displays a warning message indicating that some of the ZENworks features might behave incorrectly” on page 118
- ♦ “The Nessus scan report for ZENworks Control Center shows that the site is vulnerable to cross-site scripting attacks” on page 118

## An HTTP request is not redirected to HTTPS if IIS is running on the Primary Server

Source: ZENworks 11 SP2; ZENworks Control Center.

Explanation: During installation, the setup checks to see if the default HTTP port (80) and HTTPS port (443) are in use. If the ports are in use by another application (such as IIS), you are prompted to use alternative ports. In this case, you must access ZENworks Control Center via the port it is using and not access IIS.

Action: Although `http://Primary_Server_IP_address` works if ZENworks Control Center is using port 80, `http://Primary_Server_IP_address:###` (where ### is the port Tomcat is using) always works.

## ZENworks Control Center throws a `java.lang.NoClassDefFoundError` Exception

Source: ZENworks 11 SP2; ZENworks Control Center.

Explanation: When you use ZENworks Control Center to perform an operation, you might encounter a `java.lang.NoClassDefFoundError` exception.

Action: Restart the Novell ZENworks Server service:

**On Windows:** Do the following:

1. On the Windows desktop, click *Start > Settings > Control Panel*.
2. Double-click *Administrative Tools > Services*.
3. Restart *Novell ZENworks Server*.

**On Linux:** At the console prompt, enter `/etc/init.d/novell-zenserver restart`.

## Opening links in a new tab or new window of ZENworks Control Center might fail to display the page

Source: ZENworks 11 SP2; ZENworks Control Center.

Explanation: While browsing ZENworks Control Center, if you choose to open a link in a new tab or a new window, the page might fail to display.

Action: Open the link in the same window.

## Logging in to ZENworks Control Center or navigating within ZENworks Control Center by using Firefox 3.x might display a blank page

Source: ZENworks 11 SP2; ZENworks Control Center.

Explanation: If you are accessing ZENworks Control Center across the network by using Firefox 3.x, you might see a blank page when you log in to ZENworks Control Center or navigate within ZENworks Control Center.

Action: Do one of the following:

- ◆ Use the Firefox Web browser to open `about:config`, then change the value of `browser.cache.memory.enable` to `False`.
- ◆ Refresh the Web browser to reload the ZENworks Control Center page every time ZCC displays a blank page.
- ◆ Use any other ZENworks 11 SP2 supported Web browser to access ZENworks Control Center.

For more information about the supported Web browsers, see [“Administration Browser Requirements”](#) in the *ZENworks 11 Installation Guide*.

## ZENworks Control Center displays a warning message indicating that some of the ZENworks features might behave incorrectly

Source: ZENworks 11 SP2; ZENworks Control Center.

Explanation: When you deploy ZENworks 11 SP2 with an external database, if the Primary Server time is not synchronized with the ZENworks database server time, you might see the following warning message on the ZENworks Control Center Login page:

Some of the ZENworks features might behave incorrectly because the time of the current Primary Server and the time of the ZENworks database server are not in sync.

Action: Synchronize the Primary Server time with that of the Database Server.

## The Nessus scan report for ZENworks Control Center shows that the site is vulnerable to cross-site scripting attacks

Source: ZENworks 11 SP2; ZENworks Control Center.

Explanation: If you run a Nessus scan for the ZENworks Control Center, the report shows that the site is vulnerable to cross-site scripting attacks. This issue is addressed by the ZENworks Control Center and there is no actual vulnerability.

Action: Ignore this message. For more information, see "[User Source Authentication](#)" in the *ZENworks 11 SP2 User Source and Authentication Reference*.

